Implementation Guide

Public Health Information Network Messaging System (PHINMS)

Version: 2.8.02

Prepared by:
U.S. Department of Health & Human Services

November 1, 2012

EXECUTIVE SUMMARY

Public health involves many organizations throughout the PHIN (Public Health Information Network), working together to protect and advance the public's health. These organizations need to use the internet to securely exchange sensitive data between varieties of different public health information systems. The exchange of data, also known as "messaging" is enabled through messages created using special file formats and a standard vocabulary. The exchange uses a common approach to security and encryption, methods for dealing with a variety of firewalls, and internet protection schemes. The system provides a standard way of addressing messages being routed securely while providing a consistent confirmation of message exchange.

The Public Health Information Network Messaging System (PHINMS) sends and receives sensitive data over the internet to the public health information systems using Electronic Business Extensible Markup Language (ebXML) technology securely.

The PHINMS Implementation Guide provides instructions for installation and basic configuration of the PHINMS 2.8.02 software; advance configuration procedures are located in the PHINMS Technical Guide.

REVISION HISTORY

VERSION #	IMPLEMENTER	DATE	EXPLANATION
0.1	Lawrence Loftley	12-16-2008	Implemented 2.8.02Implementation Guide.
0.2	Tavan Jones	12-16-2008	Review
0.3	Rajeev Seenappa	12-16-2008	Review
1.0	Tom Brinks	12-17-2008	Final review and approval
1.1	Dawn Fama	11-09-2010	Revision for 2.8.01SP1release
1.2	Dawn Fama	03-20-2012	Revision for 2.8.01 HF3 release
1.3	Dawn Fama	09-28-2012	Revision for 2.8.02 release

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYM LIST

CDC	Centers for Disease Control and Prevention
CPA	Collaboration Protocol Agreement
CPS	Certification Practice Statement
ebXML	Electronic Business Extensible Markup Language
FAQs	Frequently Asked Questions
FTP	File Transfer Protocol
HF3	Hot Fix 3 (installs with 32 and 64 bit versions of java)
JDBC	Java Database Connectivity
LDAP	Lightweight Directory Access Protocol
PC	Personal Computer
PartyID	Party Identifier
PHIN	Public Health Information Network
PHINMS	Public Health Information Network Messaging System
PHINMSG	Public Health Information Network Messaging
RDBMS	Relational Database Management System
SDN	Secure Data Network
SP1	Service Pack 1
SQL	Structured Query Language
SSL	Secure Socket Layer
TLS	Transport Layer Security
TransportQ	Transport Queue
URL	Uniform Resource Locator
WorkerQ	Worker Queue

1.0 INTRODUCTION

The Public Health Information Network Messaging System (PHINMS) Implementation Guide will assist with the installation, configuration, and upgrade of the PHINMS product which is update periodically. Refer to the PHINMS website at www.cdc.gov/phin/phinms for the most current release of PHINMS software.

The PHINMS Implementation Guide provides instructions to correctly install and configure PHINMS to send and receive messages from the Centers for Disease Control and Prevention (CDC) and CDC partners. PHINMS Web Site Topics

- **Overview:** Contains a summary on the purpose of PHINMS. Announces new PHINMS features and processes.
- **Installation:** This section of the web site provides documentation pertinent to the installation and configuration the PHINMS software. Various other types of PHINMS documents are also available e.g. Acronym and Glossary List, Web Service Adapters, and many more.
- **Quick Steps:** PHINMS Quick Steps provide an overview of the information needed most often. The Quick Steps are documented for Release 2.8.02. Suggestions to add additional questions can be sent to the PHINMS Web Site point-of-contact using the Support tab.
- **FAQs:** The list of Frequently Asked Questions (FAQs) is stored in this section. The list contains answers to many questions users have previously submitted. The PHINMS Team welcomes questions, suggestions, and/or comments.
- **Support:** The Support section provides contact information for signing up to use the PHINMS Forum, contacting the Help Desk, accessing Online Help, and contacting the Web Site administrator.

1.1 References

NAME	LOCATION
Quick How Tos	Located at www.cdc.gov/phin/phinms.
PHINMS Release Notes 2.8.02	Description of supported environments, software requirements, explanation of upgrade path, and a list of new features and bug fixes made since PHINMS release 2.8.00. Located at: http://www.cdc.gov/phin/tools/PHINms/installation.html

Table 1. References

1.2 Communiqués

The PHINMS Team responds to user’s communiqués. Send questions, suggestions, and/or comments concerning PHINMS support or documentation to the PHINMS website using the Contact PHINMS email link located at the top of the home page.

2.0 INSTALLATION REQUIREMENTS

2.1 PHINMS 2.8.02 Tests

PHINMS 2.8.02 has been **tested** on the following:

- Operating systems with 32 or 64 bit version of Java installed:
  - » Windows 2003, 2008 Server (Standard or Enterprise) SP2,
  - » Windows XP SP3, Vista, Windows 7
- Certified Default Database:
  - » HSQL DB 1.8.0.4
  - » Production Qualified Databases:
  - » Microsoft SQL Server 2005,
  - » Microsoft SQL Server 2008
  - » MySQL 5.0,
  - » Oracle 10g release 2,
  - » Oracle 11g release 1,
- Application Servers:
  - » Tomcat 6.0.14,
- Proxy Servers:
  - » IIS 6.0 with Web logic 10.3 plug-in,
  - » IIS 6.0 with Jakarta Tomcat Connector 1.2.14, and
  - » IIS 7 and 7.5 with Jakarta Tomcat Connector 1.2.33

PHINMS has tested the Java Database Connectivity (JDBC) drivers to connect to the supported databases shown in Table 1. Based on the tests performed, no issues were found. PHINMS does not guarantee nor support the JDBC drivers shown below. It is up to the PHINMS customer to decide which JDBC driver to use. The table is provided for reference purposes only.

DB SERVER	VERSION	JDBC DRIVER NAME	TYPE	VERSION	DATE
MS SQL	2005	sqljdbc.jar	4	1.2.2828	10/11/2007
MS SQL	2008	Sqljdbc4.jar	4	2.0	03/25/2009
Oracle	10g Rel 2	ojdbc14.jar	4	10.2.0.2	01/22/2006
Oracle	11g Rel 1	ojdbc6.jar	4	11.1.0.7.0	08/28/2008
MySQL	5.0.67	mysql-connector-java-5.1.6-bin.jar	4	3.51.27	11/20/2008

Table 2. JDBC Drivers

2.2 System Requirements

The installation of PHINMS 2.8.02system requirements are as follows:

- Windows OS with appropriate bit version of Java installed (32-64 bit)
- 512MB of disk space,
- 1GB of memory,
- local administrator privileges, and
- System administrator privileges on Windows

Ensure all the correct ports, which may be 5088 (default local host port), 443 (Secure Socket Layer (SSL) - Hyper Text Transfer Protocol over Secure Sockets Layer (HTTPS)), and 389 (Lightweight Directory Access Protocol (LDAP)) are open on the firewall.

Once the requirements above have been met, proceed to Section 2.3, Section 2.3, and Section 2.4 can be accomplished simultaneously.

2.3 Apply for a Digital Certificate

When requesting a Digital Certificate Go to http://ca.cdc.gov and enroll in Secure Data Network. The Enrollment password is provided by the PHIN Helpdesk. Contact the PHIN helpdesk at 1-800-532-9929, to obtain a password and assistance applying for Digital Certificate. Refer to the information below to apply for the SDN PHINMS Program and Activity:

SDN PHINMS Digital Certificate Activities		
Staging	Program = "TEST"	Activity = "PHINMS 2.0"
Production	Program = "Public Health Information Network"	Activity = "PHINMS 2.0"

Table 3. SDN PHINMS Digital Certificate Activities

2.4 Request PartyID

To obtain the PHINMS software, email the PHIN Help Desk PHINTech@cdc.gov. Information will be required about the organization(s) sending and/or receiving messages. The information will be reviewed and confirmed by a PHINMS support team member and the software download link with a PHINMS PartyID will be emailed to the requestor. Contact the PHIN Help Desk regarding any issues encountered with the PartyID, by sending an email to PHINTech@cdc.gov.

A unique PartyID is required for each organization and every organization sending and receiving messages to the CDC. A PartyID uniquely identifies a PHINMS installation, also called an instance or node. The PartyID is included with every message informing the recipient of the originator.

The PartyID is required during installation and becomes a permanent, identifying part of the application. The PHINMS application will need to be reinstalled if the PartyID needs to be changed.

Note: When a need to install PHINMS at more than one site or to install more than one PHINMS installation at the same site, a unique PartyID is required for each installation.

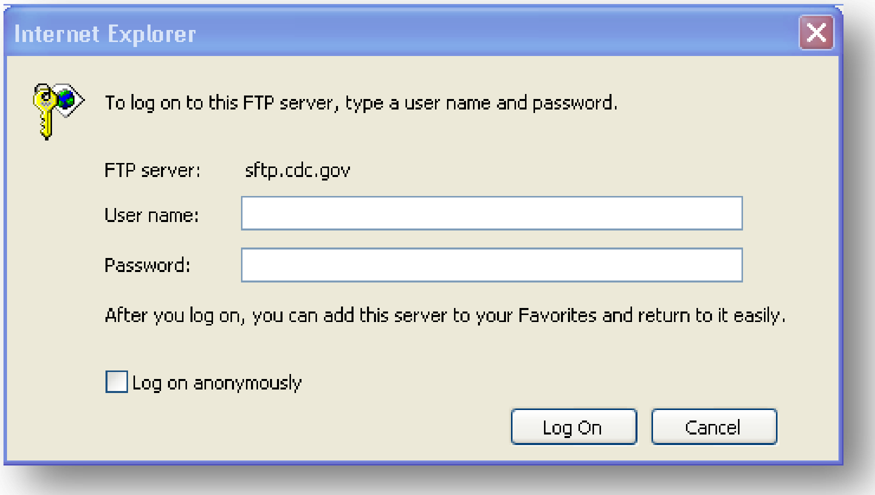
The recommended way to install PHINMS 2.8.02 is to download the application from the File Transport Site (FTP) site.

3.0 DOWNLOAD & INSTALL THE PHINMS SOFTWARE

Install the PHINMS 2.8.02 following the steps below:

Note: Refer to Section 2.4 if an email was not received with the PartyID information.

1. Navigate to **ftp://sftp.cdc.gov** displaying Figure 3.1,



To log on to this FTP server, type a user name and password.

FTP server: sftp.cdc.gov

User name:

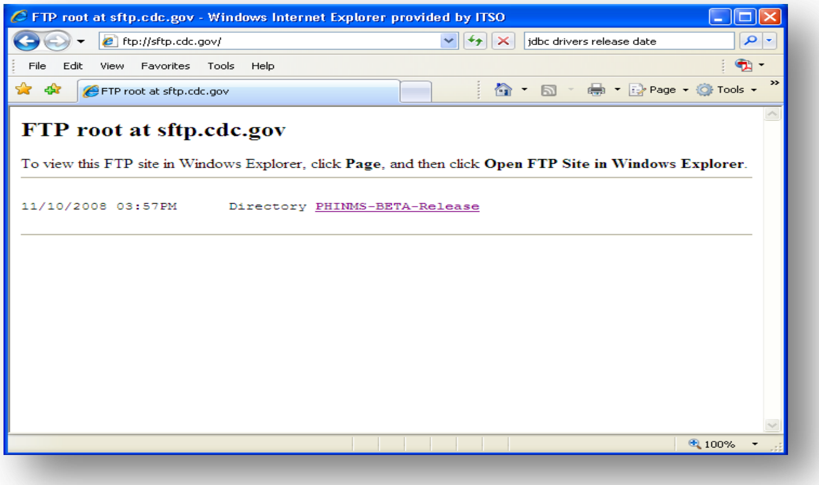
Password:

After you log on, you can add this server to your Favorites and return to it easily.

□ Log on anonymously

Figure 3.1. Log On As

2. Enter User name, Password, select LogOn displaying Figure 3.1,



FTP root at sftp.cdc.gov - Windows Internet Explorer provided by ITSO
ftp://sftp.cdc.gov/
jdbc drivers release date
File
Edit
View
Favorites
Tools
Help
FTP root at sftp.cdc.gov
Page
Tools
100%

FTP root at sftp.cdc.gov

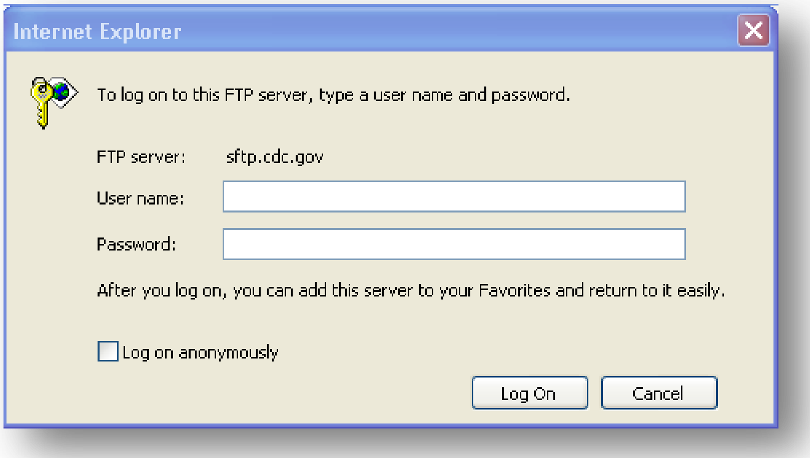
To view this FTP site in Windows Explorer, click **Page**, and then click **Open FTP Site in Windows Explorer**.

```
11/10/2008 03:57PM      Directory PHINMS-BETA-Release
```

Figure 3.2. Phinms 2.8.02 FTP downloads

3. To view this FTP site in Windows Explorer, enter the link in the Explorer bar and select enter. displaying Figure 3.2,

4. Enter User name, Password, select LogOn displaying Figure 3.3,



Internet Explorer

To log on to this FTP server, type a user name and password.

FTP server: sftp.cdc.gov

User name:

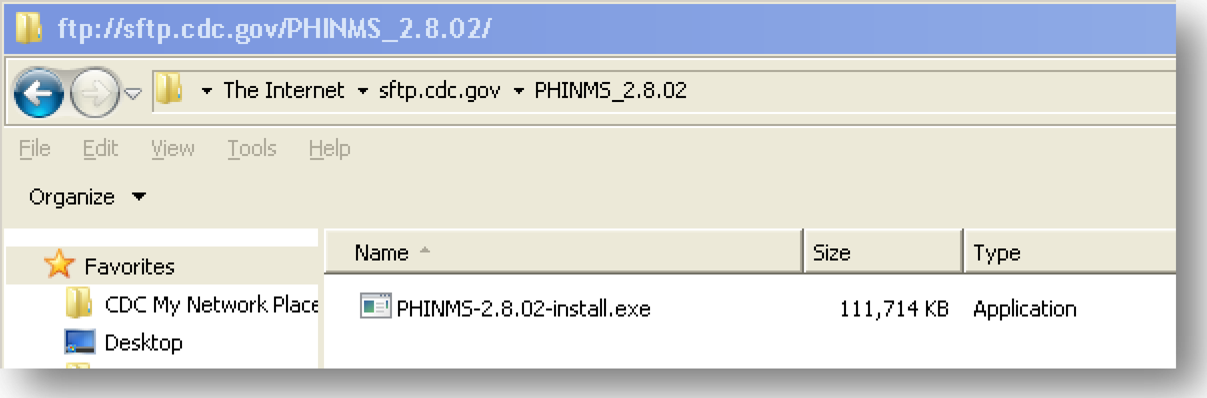
Password:

After you log on, you can add this server to your Favorites and return to it easily.

□ Log on anonymously

Figure 3.3. FTP log on

5. Select the PHINMS 2.8.02 folder, displayed in Figure 3.4,

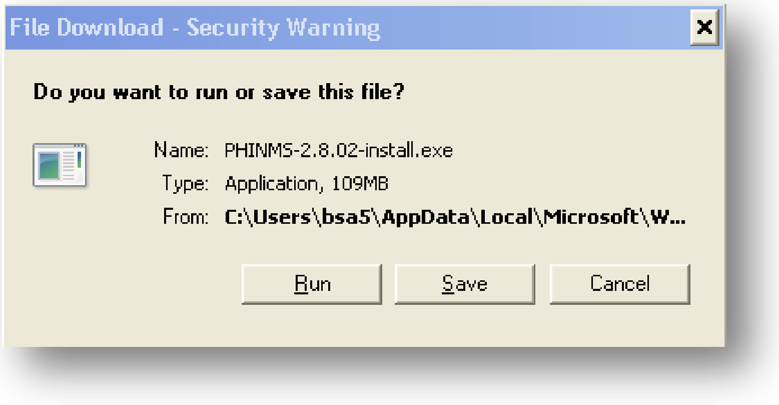


ftp://sftp.cdc.gov/PHINMS_2.8.02/

Name	Size	Type
PHINMS-2.8.02-install.exe	111,714 KB	Application

Figure 3.4. Phinms 2.8.02 FTP Windows Build

6. Double-click on PHINMS-2.8.02-install.exe file displaying Figure 3.5,



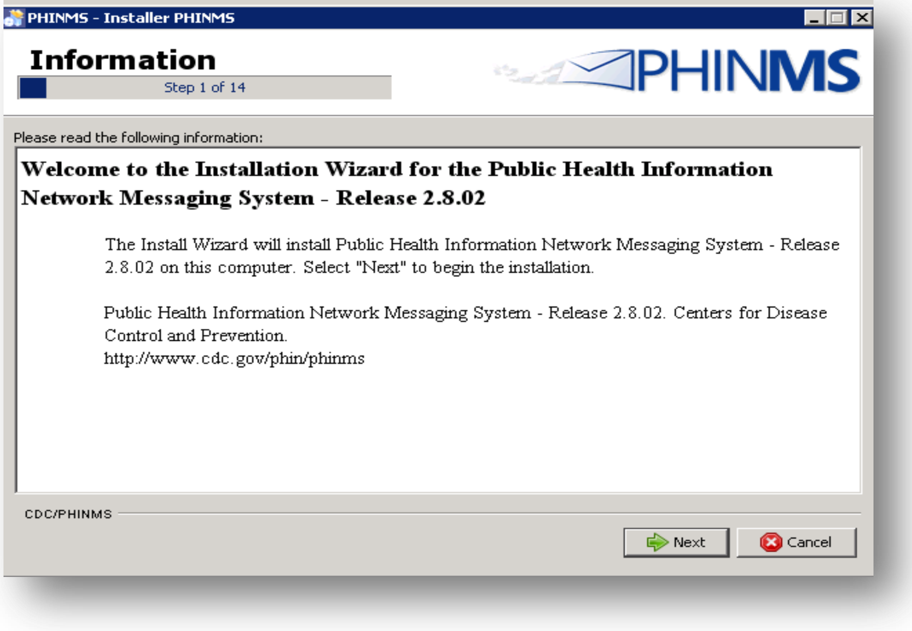
File Download - Security Warning

Do you want to run or save this file?

Name: PHINMS-2.8.02-install.exe
Type: Application, 109MB
From: C:\Users\bsa5\AppData\Local\Microsoft\W...

Figure 3.5. File Download - Security Warning

7. Select Save, to save the application to your local computer and double-click PHINMS-2.8.02 -install.exe,



PHINMS - Installer PHINMS

Information

Step 1 of 14

Please read the following information:

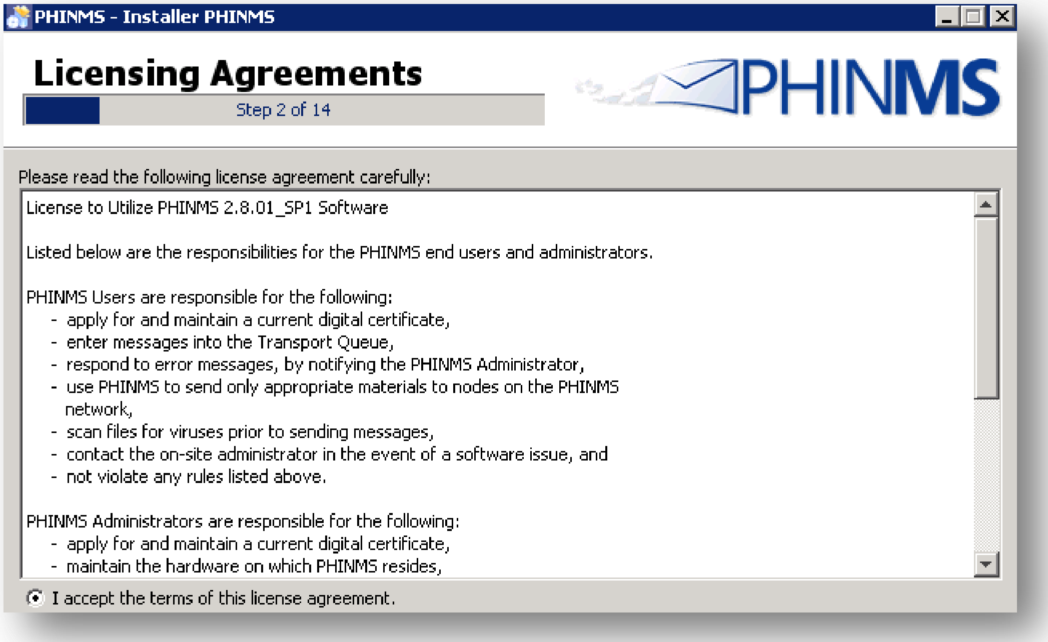
Welcome to the Installation Wizard for the Public Health Information Network Messaging System - Release 2.8.02

The Install Wizard will install Public Health Information Network Messaging System - Release 2.8.02 on this computer. Select "Next" to begin the installation.

Public Health Information Network Messaging System - Release 2.8.02. Centers for Disease Control and Prevention.
http://www.cdc.gov/phin/phinms

Figure 3.6. Install Shield Wizard Preparation Screens

8. Select Next displaying Figure 3.6,



PHINMS - Installer PHINMS

Licensing Agreements

Step 2 of 14

Please read the following license agreement carefully:

License to Utilize PHINMS 2.8.01_SP1 Software

Listed below are the responsibilities for the PHINMS end users and administrators.

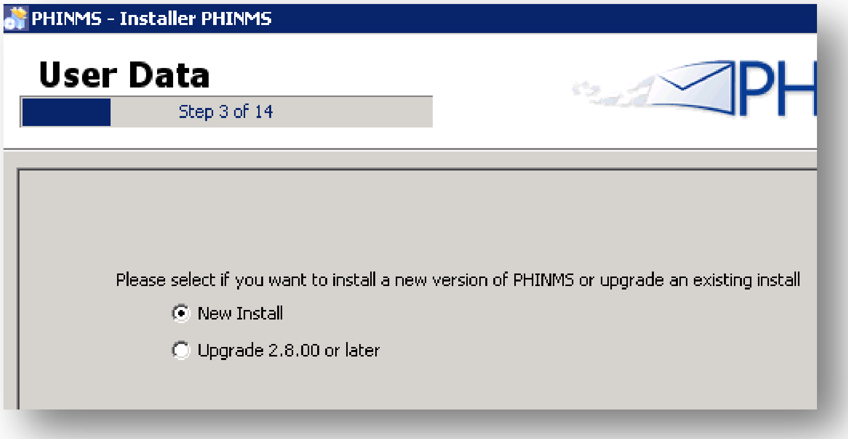
PHINMS Users are responsible for the following:
- apply for and maintain a current digital certificate,
- enter messages into the Transport Queue,
- respond to error messages, by notifying the PHINMS Administrator,
- use PHINMS to send only appropriate materials to nodes on the PHINMS network,
- scan files for viruses prior to sending messages,
- contact the on-site administrator in the event of a software issue, and
- not violate any rules listed above.

PHINMS Administrators are responsible for the following:
- apply for and maintain a current digital certificate,
- maintain the hardware on which PHINMS resides,

● I accept the terms of this license agreement.

Figure 3.7. End User Agreement Screen

9. Select I accept the terms of the license agreement, select Next displaying Figure 3.7,



PHINMS - Installer PHINMS

User Data

Step 3 of 14

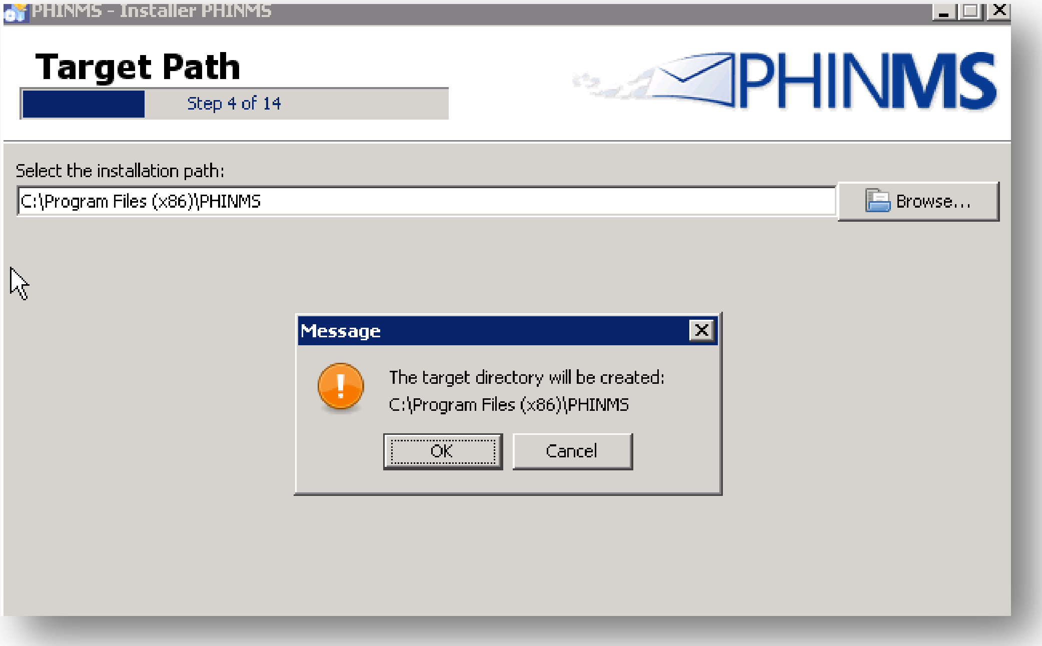
Please select if you want to install a new version of PHINMS or upgrade an existing install

● New Install

○ Upgrade 2.8.00 or later

Figure 3.8. New Installation or Upgrade Screen

10. Select New PHINMS Installation, displaying in Figure 3.8,
11. Select Ok to select the default directory or Browse to install to a different directory, displaying Figure 3.9,



PHINMS - Installer PHINMS

Target Path

Step 4 of 14

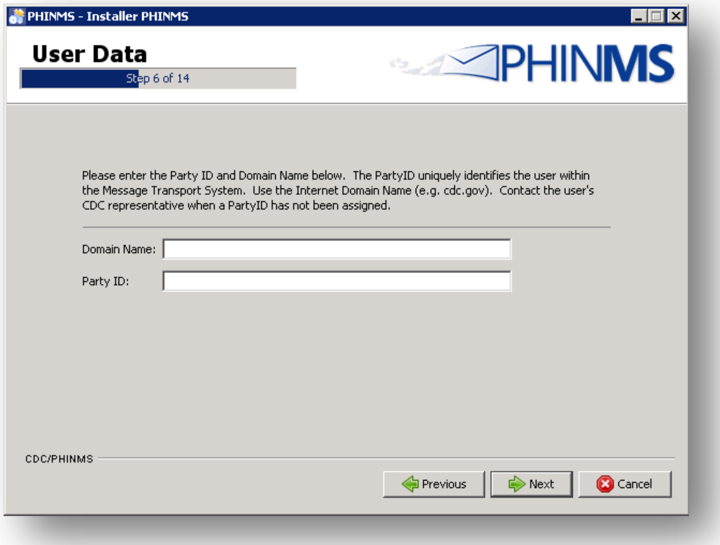
Select the installation path:

C:\Program Files (x86)\PHINMS

Message

The target directory will be created:
C:\Program Files (x86)\PHINMS

Figure 3.9. The target directory will be created



PHINMS - Installer PHINMS

User Data

Step 6 of 14

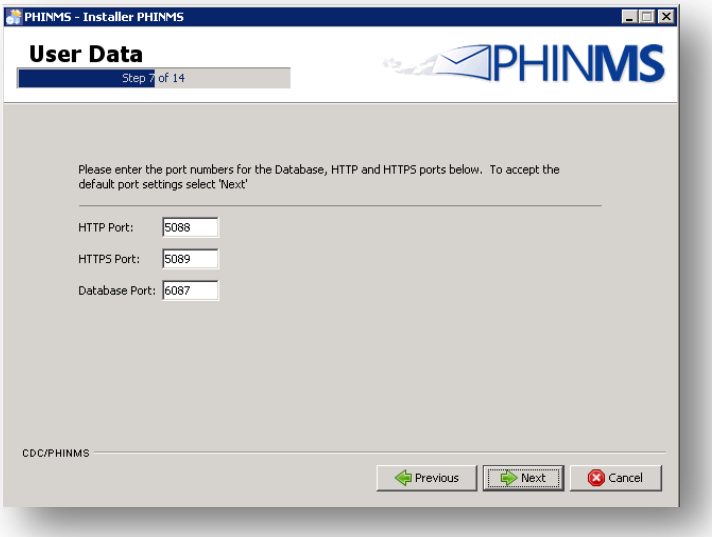
Please enter the Party ID and Domain Name below. The PartyID uniquely identifies the user within the Message Transport System. Use the Internet Domain Name (e.g. cdc.gov). Contact the user's CDC representative when a PartyID has not been assigned.

Domain Name:

Party ID:

Figure 3.10. PartyID and Domain Name Screen

12. Enter the PartyID and Domain Name, select Next displaying Figure 3.10,


PHINMS - Installer PHINMS

User Data

Step 7 of 14

Please enter the port numbers for the Database, HTTP and HTTPS ports below. To accept the default port settings select 'Next'

HTTP Port: 5088

HTTPS Port: 5089

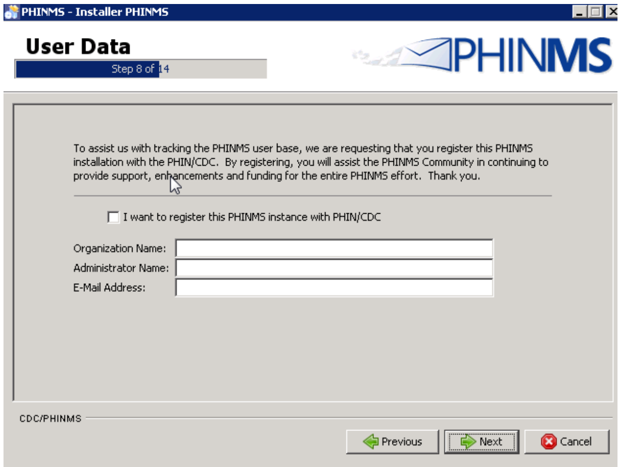
Database Port: 6087

Figure 3.11. Port Numbers Screen

Note: The PHINMS default port numbers are 6087 for the Database, 5088 for HTTP, and 5089 for HTTPS.

13. Select Next displaying Figure 3.12 then the registration screen displays, It is optional to enter Business/Organization Name, Name, Email to register the product with the CDC,

Note: Currently there is no active registration server. It is advised to not check the box.


PHINMS - Installer PHINMS

User Data

Step 8 of 14

To assist us with tracking the PHINMS user base, we are requesting that you register this PHINMS installation with the PHIN/CDC. By registering, you will assist the PHINMS Community in continuing to provide support, enhancements and funding for the entire PHINMS effort. Thank you.

□ I want to register this PHINMS instance with PHIN/CDC

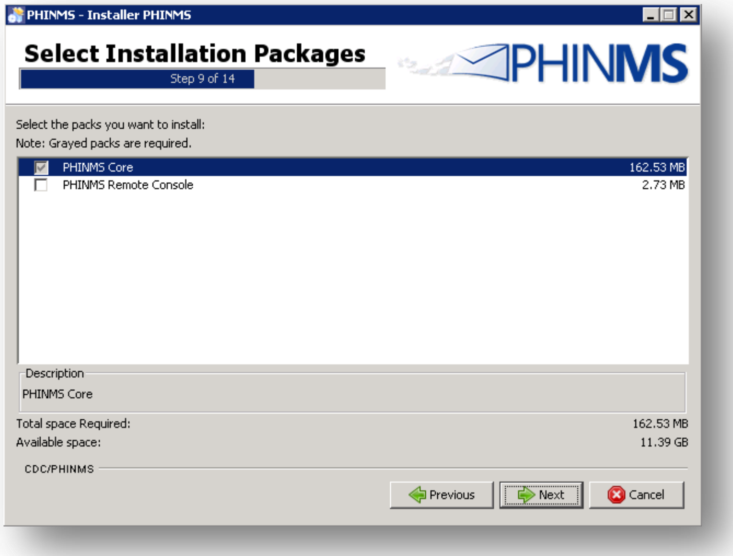
Organization Name:

Administrator Name:

E-Mail Address:

Figure 3.12. Register this PHINMS instance with PHIN/CDC

14. Select Next for PHINMS Core only. Displaying Figure 3.13,



Select Installation Packages

Step 9 of 14

Select the packs you want to install:
Note: Grayed packs are required.

☑	PHINMS Core	162.53 MB
□	PHINMS Remote Console	2.73 MB

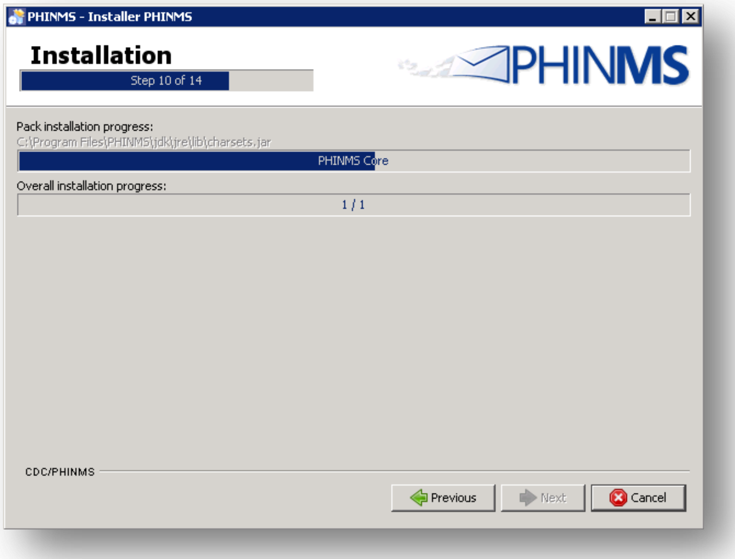
Description
PHINMS Core

Total space Required: 162.53 MB
Available space: 11.39 GB

CDC/PHINMS

Figure 3.13. Installation Package screen

15. Select Next displaying Figure 3.14,



Installation

Step 10 of 14

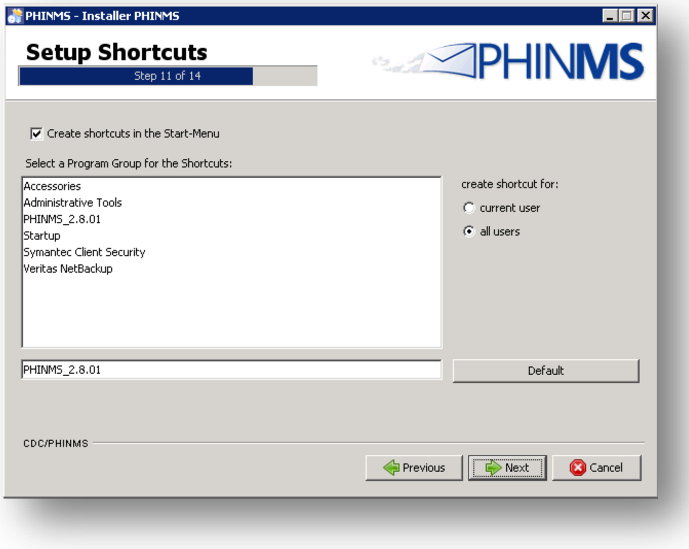
Pack installation progress:
C:\Program Files\PHINMS\jdk\jre\lib\charsets.jar
PHINMS Core

Overall installation progress:
1 / 1

CDC/PHINMS

Figure 3.14. Installation

16. Select Next displaying Figure 3.15,



PHINMS - Installer PHINMS

Setup Shortcuts

Step 11 of 14

☑ Create shortcuts in the Start-Menu

Select a Program Group for the Shortcuts:

Accessories
Administrative Tools
PHINMS_2.8.01
Startup
Symantec Client Security
Veritas NetBackup

create shortcut for:

○ current user

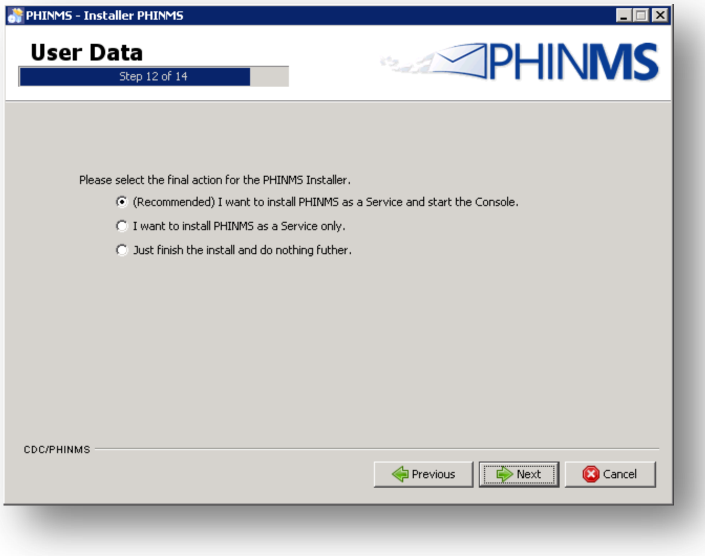
● all users

PHINMS_2.8.01

Figure 3.15. Setup Shortcuts

Note: Select where the shortcut should be created, if you choose to relocate the shortcut while on this screen after your first choice has been made, choose default to reset this screen.

17. Select Next displaying Figure 3.16,



PHINMS - Installer PHINMS

User Data

Step 12 of 14

Please select the final action for the PHINMS Installer.

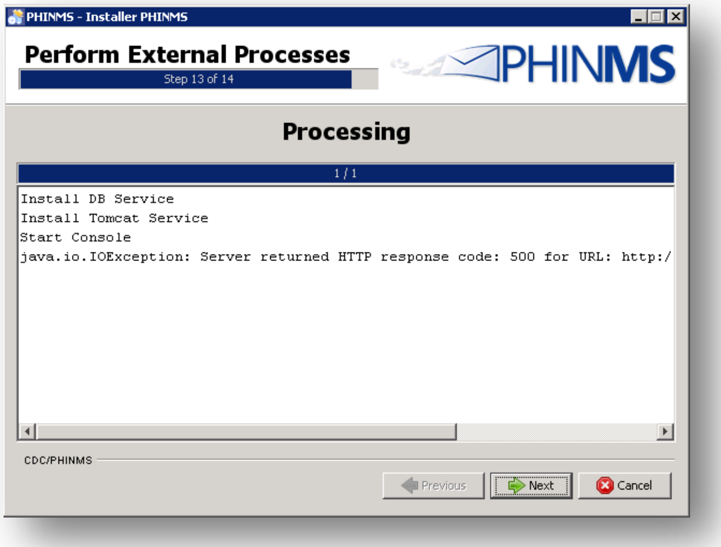
● (Recommended) I want to install PHINMS as a Service and start the Console.

○ I want to install PHINMS as a Service only.

○ Just finish the install and do nothing futher.

Figure 3.16. PHINMS Installation Options

18. Select how PHINMS is to be installed (i.e., as a Service and start Console, Service only, or not as a Service). Select Next displaying Figure 3.17,



```
Install DB Service
Install Tomcat Service
Start Console
java.io.IOException: Server returned HTTP response code: 500 for URL: http:/
```

Figure 3.17. PHINMS Processing

19. Select Done to initiate PHINMS for the first time, displaying Figure 3.18,

Note: The console may appear in front of the Installation Finished window.

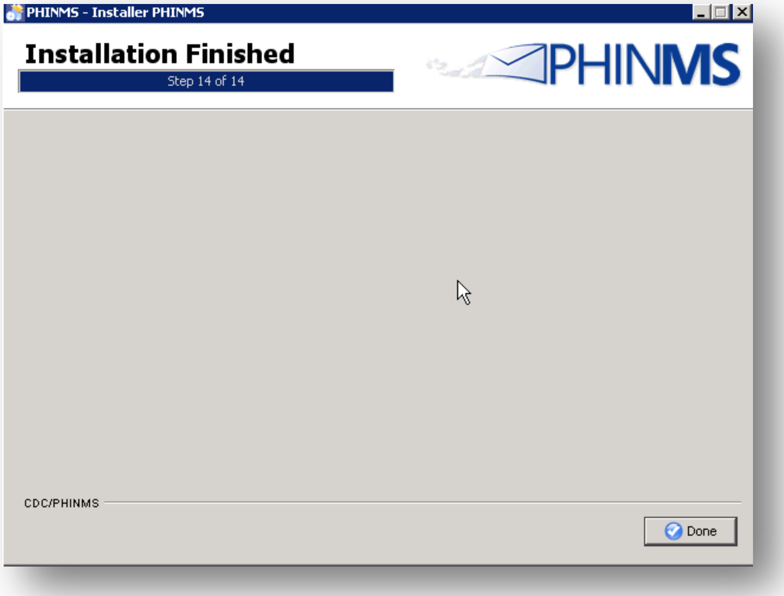
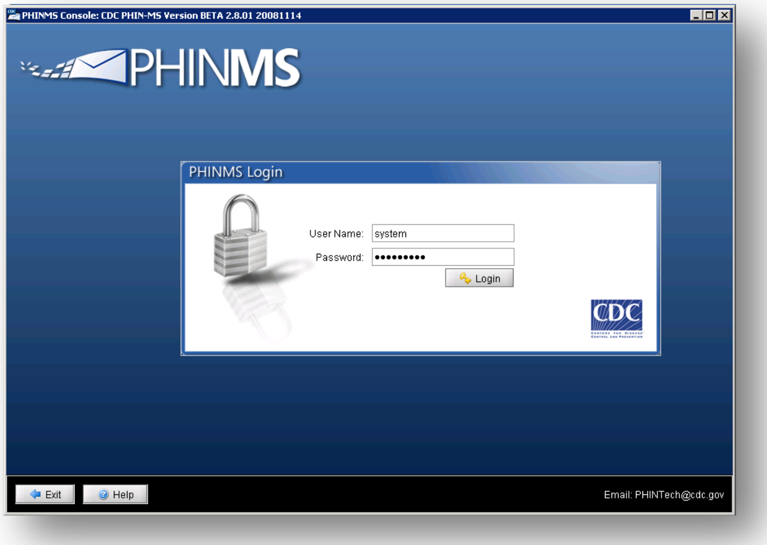


Figure 3.18. PHINMS Installation Finished

20. PHINMS Console login screen comes up, displaying Figure 3.19.



PHINMS Console: CDC PHIN-MS Version BETA 2.8.01 20081114

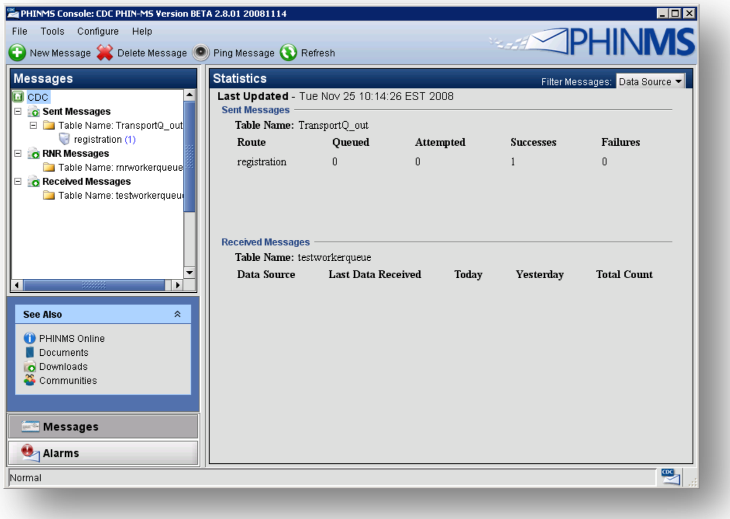
PHINMS Login

User Name: system

Password: •••••••••

Figure 3.19. PHINMS Console Login Screen

21. Enter Username = system and Password = Phinms123 then click Login, displaying Figure 3.20,



PHINMS Console: CDC PHIN-MS Version BETA 2.8.01 20081114

Statistics

Filter Messages: Data Source

Last Updated - Tue Nov 25 10:14:26 EST 2008

Sent Messages

Table Name: TransportQ_out

Route	Queued	Attempted	Successes	Failures
registration	0	0	1	0

Received Messages

Table Name: testworkerqueue

Data Source	Last Data Received	Today	Yesterday	Total Count

Figure 3.20. PHINMS Console

4.0 UPGRADE PHINMS SOFTWARE

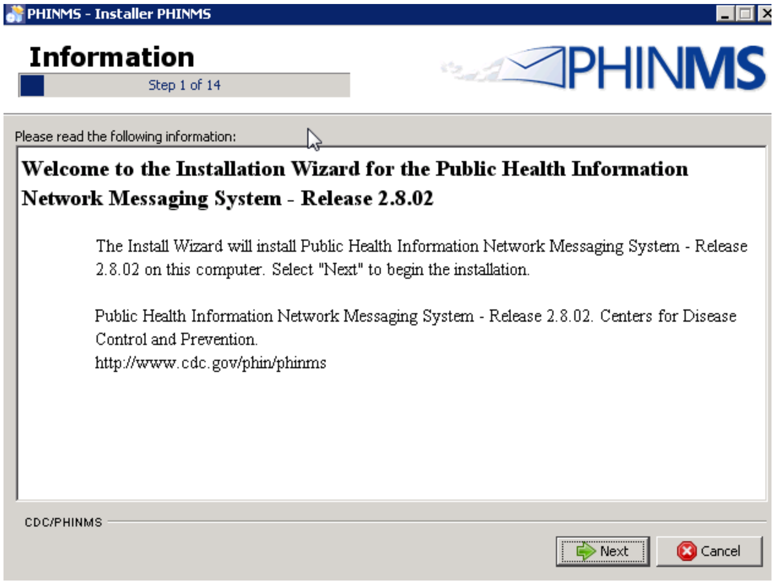
PHINMS 2.8.02 allows the user to upgrade from version 2.8.00 and PHINMS 2.8.01, SP1, HF2, and HF3 only. Prior versions of the PHINMS software will be required to perform a fresh install of PHINMS 2.8.02.

Note: The PHINMS upgrade will not overwrite the previous versions. It will install PHINMS 2.8.02 in a new location and pull the configuration files, mainly the TransportQ table configuration information and use this information to configure the new PHINMS 2.8.02 application. This allows the user to have the previous installation intact if there are any problems.

Complete the following steps to upgrade to version 2.8.02 from versions 2.8.00 through HF3:

PLEASE FOLLOW THESE STEPS CAREFULLY

1. Close the console for the previous version of PHINMS,
2. Stop the PHINMS services for the previous version of PHINMS (Windows Services),
3. Rename the existing instance of PHINMS to PHINMSold,
4. Open the executable file PHINMS-2.8.02-install.exe displaying Figure 4.1, the Install Wizard will take a few moments displaying in Figure 4.1,



PHINMS - Installer PHINMS

Information

Step 1 of 14

Please read the following information:

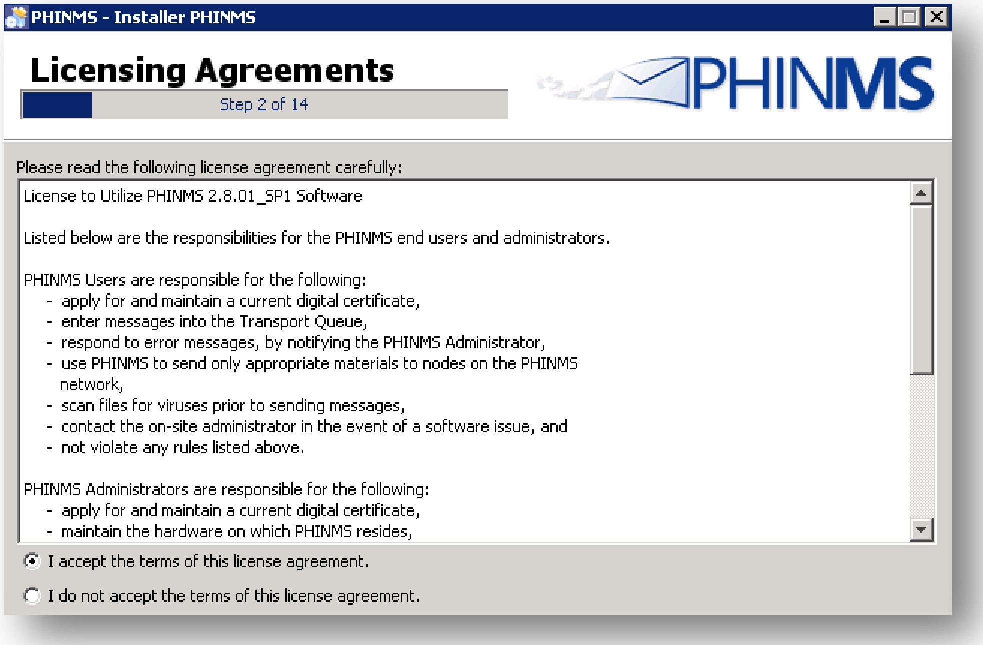
Welcome to the Installation Wizard for the Public Health Information Network Messaging System - Release 2.8.02

The Install Wizard will install Public Health Information Network Messaging System - Release 2.8.02 on this computer. Select "Next" to begin the installation.

Public Health Information Network Messaging System - Release 2.8.02. Centers for Disease Control and Prevention.
http://www.cdc.gov/phin/phinms

Figure 4.1. Install Shield Wizard Preparation Screens

5. Select Next displaying Figure 4.2,



Please read the following license agreement carefully:

License to Utilize PHINMS 2.8.01_SP1 Software

Listed below are the responsibilities for the PHINMS end users and administrators.

PHINMS Users are responsible for the following:
- apply for and maintain a current digital certificate,
- enter messages into the Transport Queue,
- respond to error messages, by notifying the PHINMS Administrator,
- use PHINMS to send only appropriate materials to nodes on the PHINMS network,
- scan files for viruses prior to sending messages,
- contact the on-site administrator in the event of a software issue, and
- not violate any rules listed above.

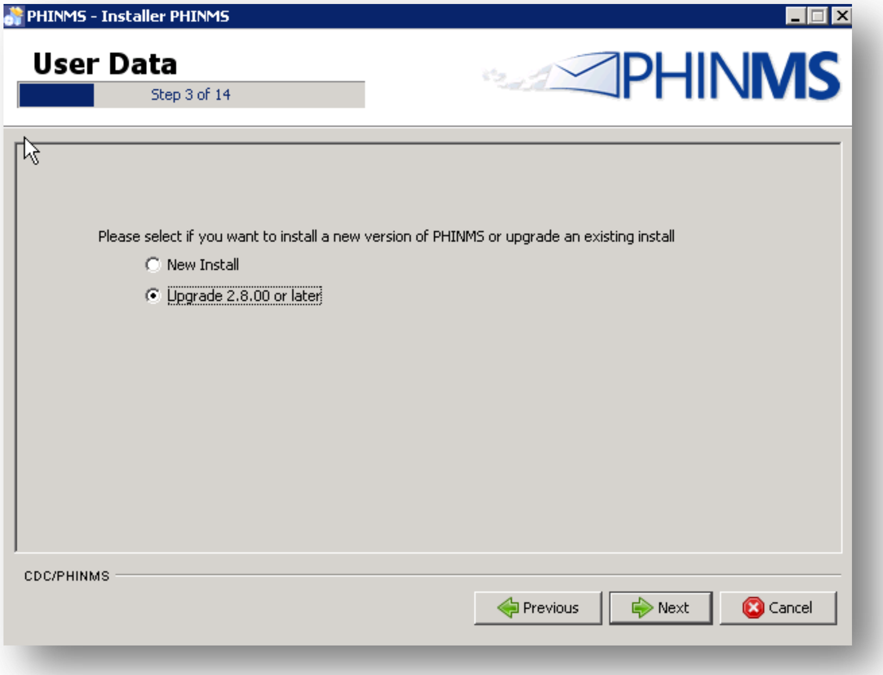
PHINMS Administrators are responsible for the following:
- apply for and maintain a current digital certificate,
- maintain the hardware on which PHINMS resides,

● I accept the terms of this license agreement.

○ I do not accept the terms of this license agreement.

Figure 4.2. End User Agreement Screen

6. Select I accept the terms of the license agreement,



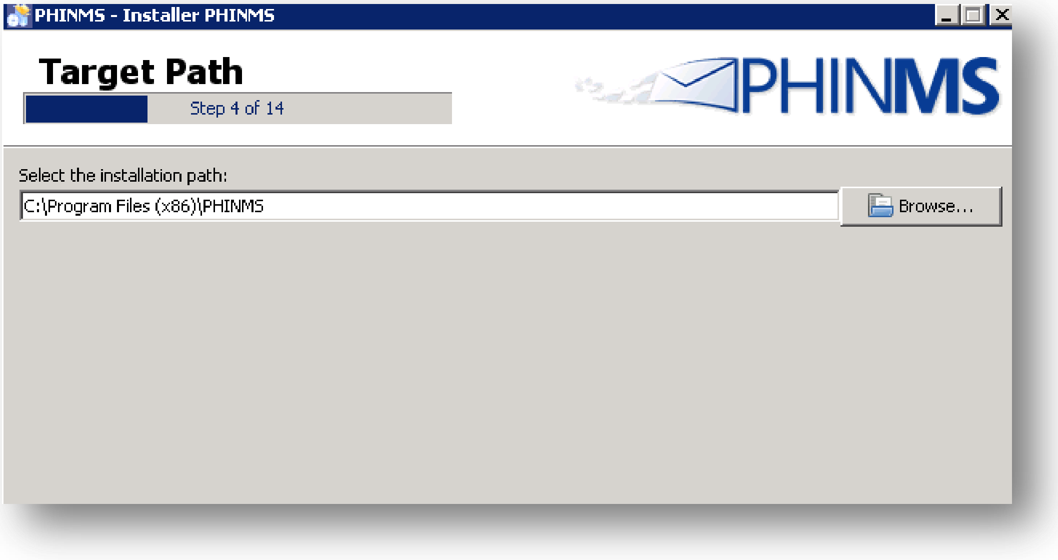
Please select if you want to install a new version of PHINMS or upgrade an existing install

○ New Install

● Upgrade 2.8.00 or later

Figure 4.3. New Installation or Upgrade Screen

7. Select Upgrade PHINMS Software, Next displaying Figure 4.3,



PHINMS - Installer PHINMS

Target Path

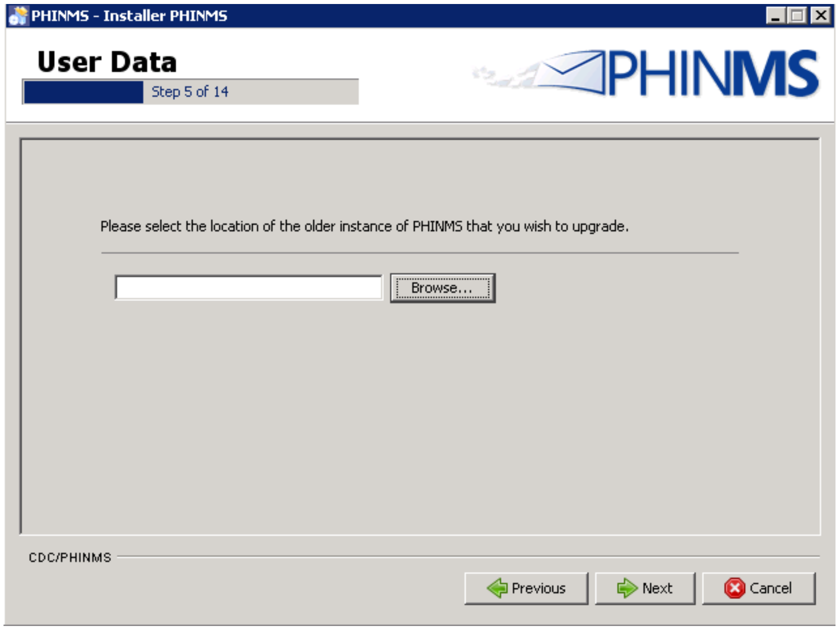
Step 4 of 14

Select the installation path:

C:\Program Files (x86)\PHINMS

Figure 4.4. The target directory will be created

8. Make sure the install path is the <u>same path as the previous version</u> **before** renaming the directory to PHINMSold,
9. Select Next,
10. Browse to the location of the older instance of PHINMS Ex: PHINMSold,



PHINMS - Installer PHINMS

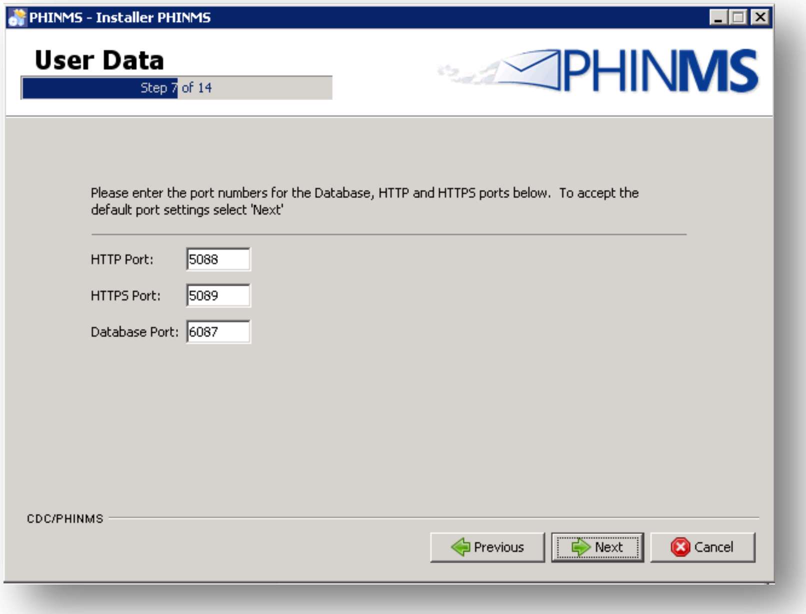
User Data

Step 5 of 14

Please select the location of the older instance of PHINMS that you wish to upgrade.

Figure 4.5 The Upgrade location

11. Select Next displaying Figure 4.6,



PHINMS - Installer PHINMS

User Data

Step 7 of 14

Please enter the port numbers for the Database, HTTP and HTTPS ports below. To accept the default port settings select 'Next'

HTTP Port: 5088

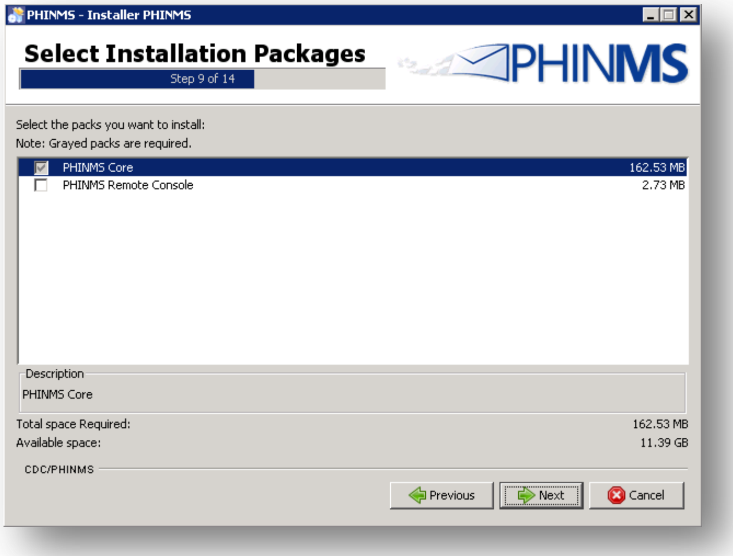
HTTPS Port: 5089

Database Port: 6087

Figure 4.6. Port Numbers Screen

Note: The PHINMS default port numbers are 6087 for the Database, 5088 for HTTP, and 5089 for HTTPS.

12. Select Next displaying Figure 4.7 then the Installation Package screen,



PHINMS - Installer PHINMS

Select Installation Packages

Step 9 of 14

Select the packs you want to install:
Note: Grayed packs are required.

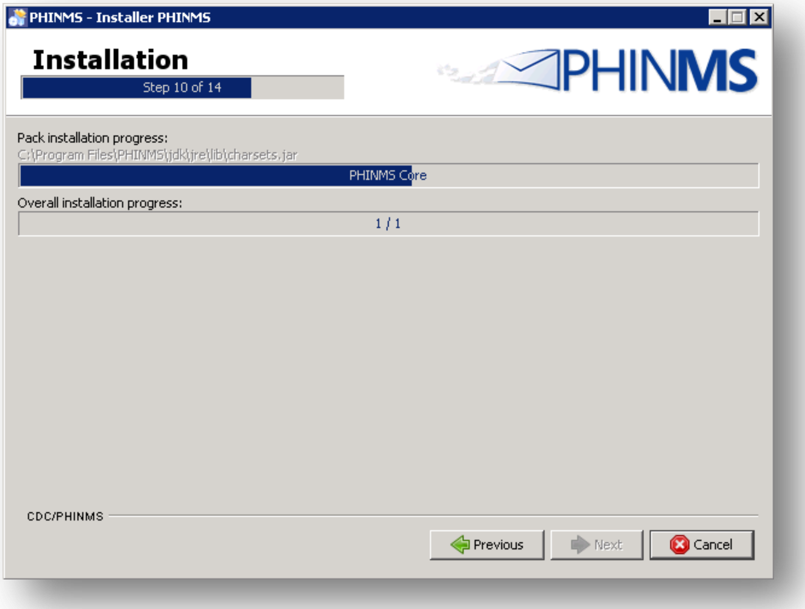
☑ PHINMS Core 162.53 MB
□ PHINMS Remote Console 2.73 MB

Description
PHINMS Core

Total space Required: 162.53 MB
Available space: 11.39 GB

Figure 4.7. Installation Package screen

13. Select Next displaying Figure 4.8,



Installation

Step 10 of 14

Pack installation progress:

C:\Program Files\PHINMS\jdk\jre\lib\charsets.jar

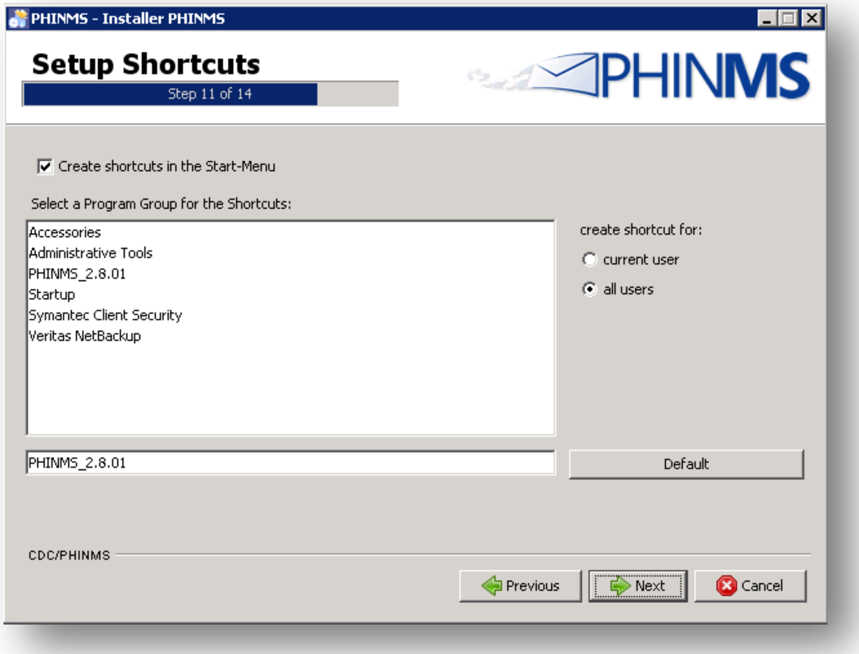
PHINMS Core

Overall installation progress:

1 / 1

Figure 4.8. Installation

14. Select Next displaying Figure 4.9,



Setup Shortcuts

Step 11 of 14

☑ Create shortcuts in the Start-Menu

Select a Program Group for the Shortcuts:

Accessories
Administrative Tools
PHINMS_2.8.01
Startup
Symantec Client Security
Veritas NetBackup

PHINMS_2.8.01

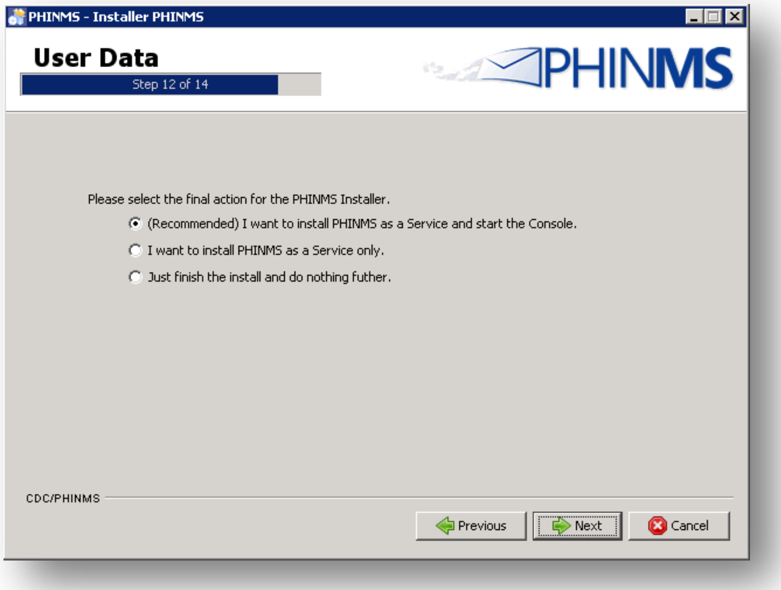
create shortcut for:

○ current user

● all users

Figure 4.9. Setup Shortcuts

15. Select where the shortcut should be created, if you choose to relocate the shortcut while on this screen after your first choice has been made, choose default to reset this screen.



Please select the final action for the PHINMS Installer.

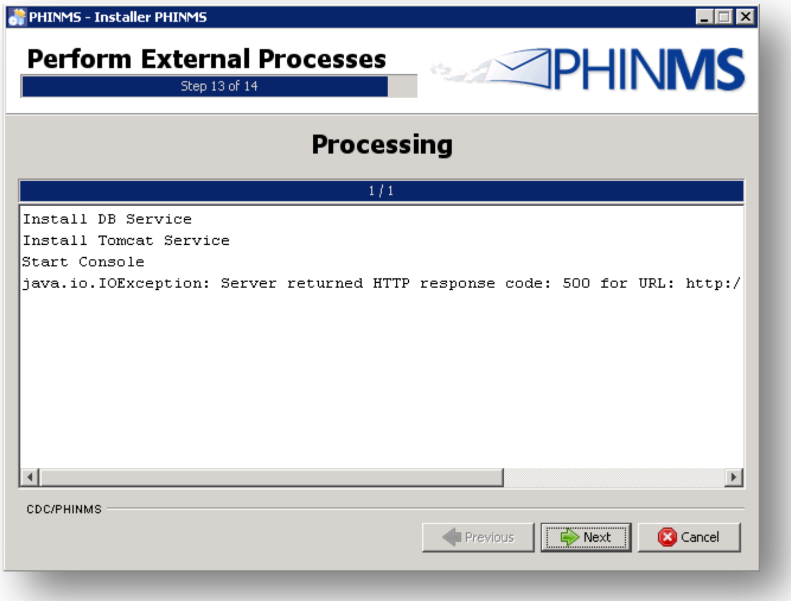
● (Recommended) I want to install PHINMS as a Service and start the Console.

○ I want to install PHINMS as a Service only.

○ Just finish the install and do nothing futher.

Figure 4.10. PHINMS Installation Options

16. Select how PHINMS is to be installed (i.e., as a Service and start Console, Service only, or not as a Service),



```
Install DB Service
Install Tomcat Service
Start Console
java.io.IOException: Server returned HTTP response code: 500 for URL: http:/
```

Figure 4.11. PHINMS Processing

17. Select Next displaying Figure 4.11,

Note: The console may open infront of the screen capture below.

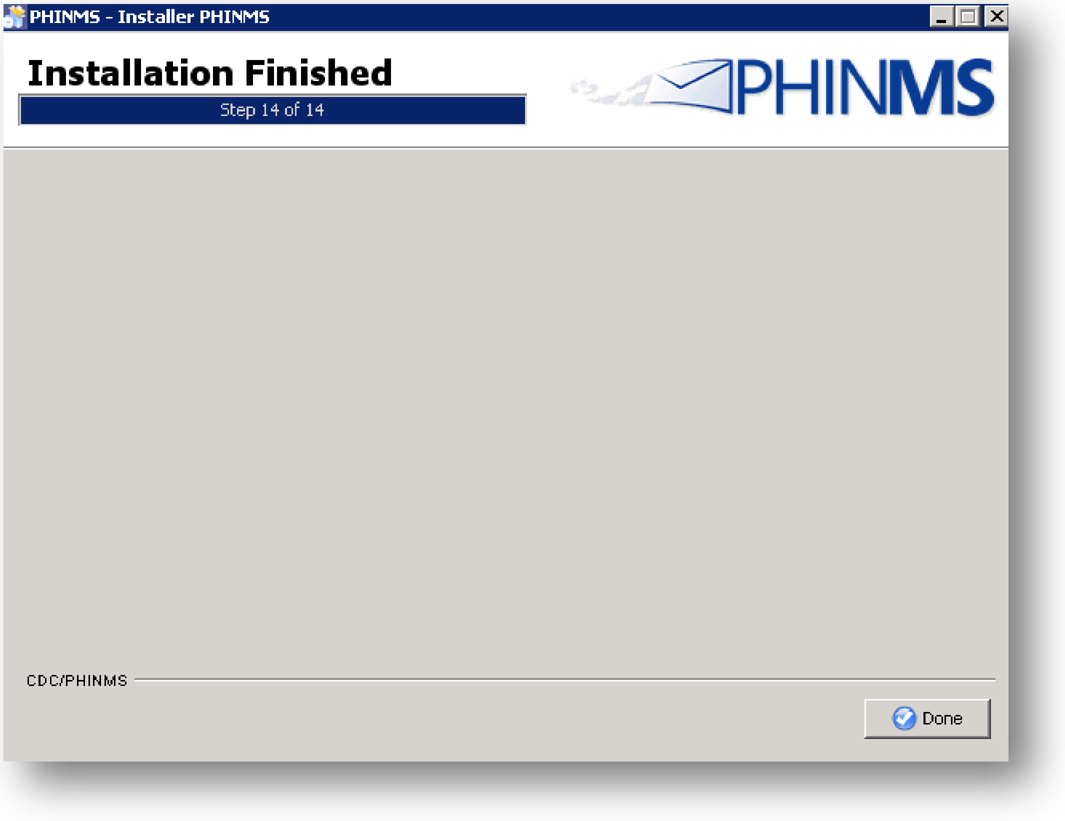
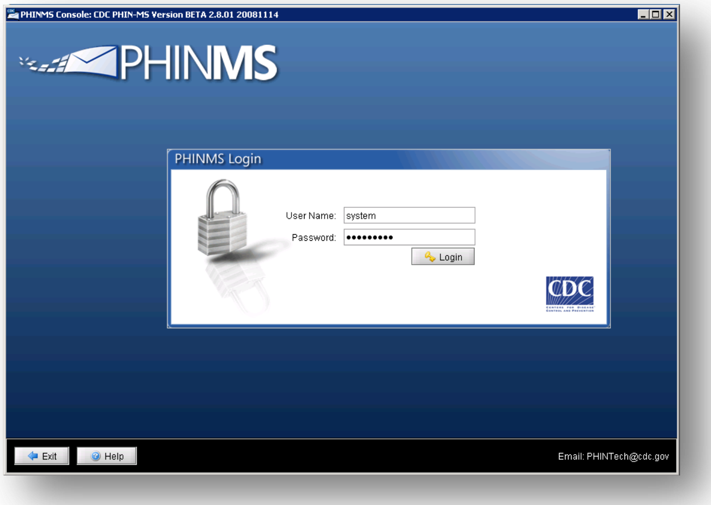


Figure 4.12. PHINMS Installation Finished

Note: The installation has been completed successfully. An uninstaller has been created. There is now an option to generate an automatic installation script to deploy PHINMS with the same configuration on another system.

18. Select Done,
19. PHINMS Console login screen comes up, displaying Figure 4.13, and



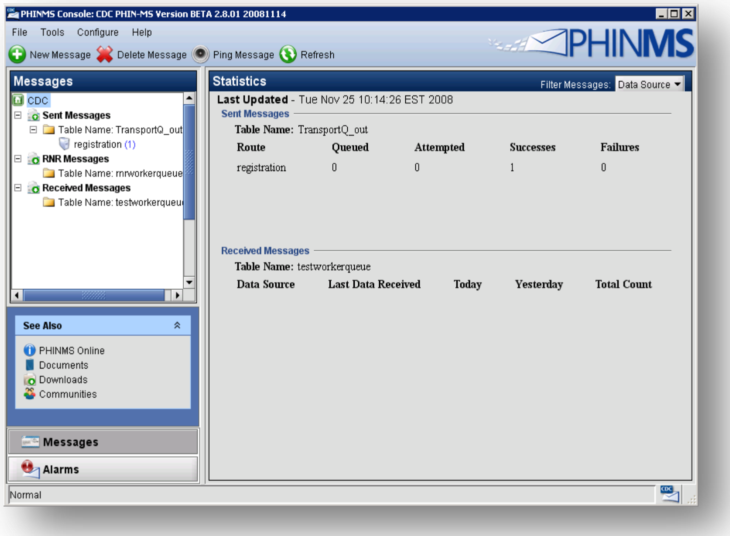
User Name: system

Password: •••••••••

Login

Figure 4.13. PHINMS Console Login Screen

20. Enter Username and Password the click Login, displaying Figure 4.14.



Statistics

Filter Messages: Data Source

Last Updated - Tue Nov 25 10:14:26 EST 2008

Sent Messages

Table Name: TransportQ_out

Route	Queued	Attempted	Successes	Failures
registration	0	0	1	0

Received Messages

Table Name: testworkerqueue

Data Source	Last Data Received	Today	Yesterday	Total Count

Figure 4.14. PHINMS Console

5.0 CONFIGURE SQL DATABASES

A Structured Query Language (HSQLDB) database containing a Transport Queue (TransportQ) is automatically installed with the PHINMS 2.8.02application. An external database can be created for the purpose of hosting the messaging queue tables. PHINMS 2.8.02will support the following databases for hosting messaging queues:

- HSQLDB 1.8.0.
- Microsoft SQL Server 2005 and 2008
- MySQL 5.0,
- Oracle 10g and 11g.

A HSQL database is provided with the PHINMS installation on the Windows platform as a default database and facilitates testing installation. Evaluation of the tradeoffs between SQL and a high transaction volume Relational Database Management System (RDBMS) such as others listed above is recommended.

All Table scripts needed for PHINMS external database configurations for the databases listed above will be posted on the FTP site (ftp://sftp.cdc.gov/PHINMS). The provided table scripts are for the Transport Queue, Worker Queue only.

Note: To use an external Database (DB) connection, the appropriate JDBC driver must be imported into PHINMS via the PHINMS Console Tools option (section 9.6). DB drivers can also be found on the ftp site (ftp://sftp.cdc.gov/PHINMS/PHINMS_Database_Drivers/)

For external DB connection string properties, please refer to the *PHINMS Technical Guide*

6.0 SENDER INFORMATION

PHINMS Version 2.8.02installation has two components - the Sender and the Receiver. Sending a test message allows the PHINMS Sender to send messages to the TransportQ and to the CDC. Testing the PHINMS installation is a three-part procedure which includes the following:

- ping the PHINMS Sender loopback route,
- ping a configured PHINMS Route. (Requires Collaboration Protocol Agreement (CPA) files have been imported on the receiving side)
- ping the PHINMS CDC Staging Receiver. (Requires Collaboration Protocol Agreement (CPA) files be emailed to Phintech@cdc.gov. Refer to Section 6.4 for more information.

Figure 6.1 displays a diagram to assist with understanding the PHINMS authentication process.

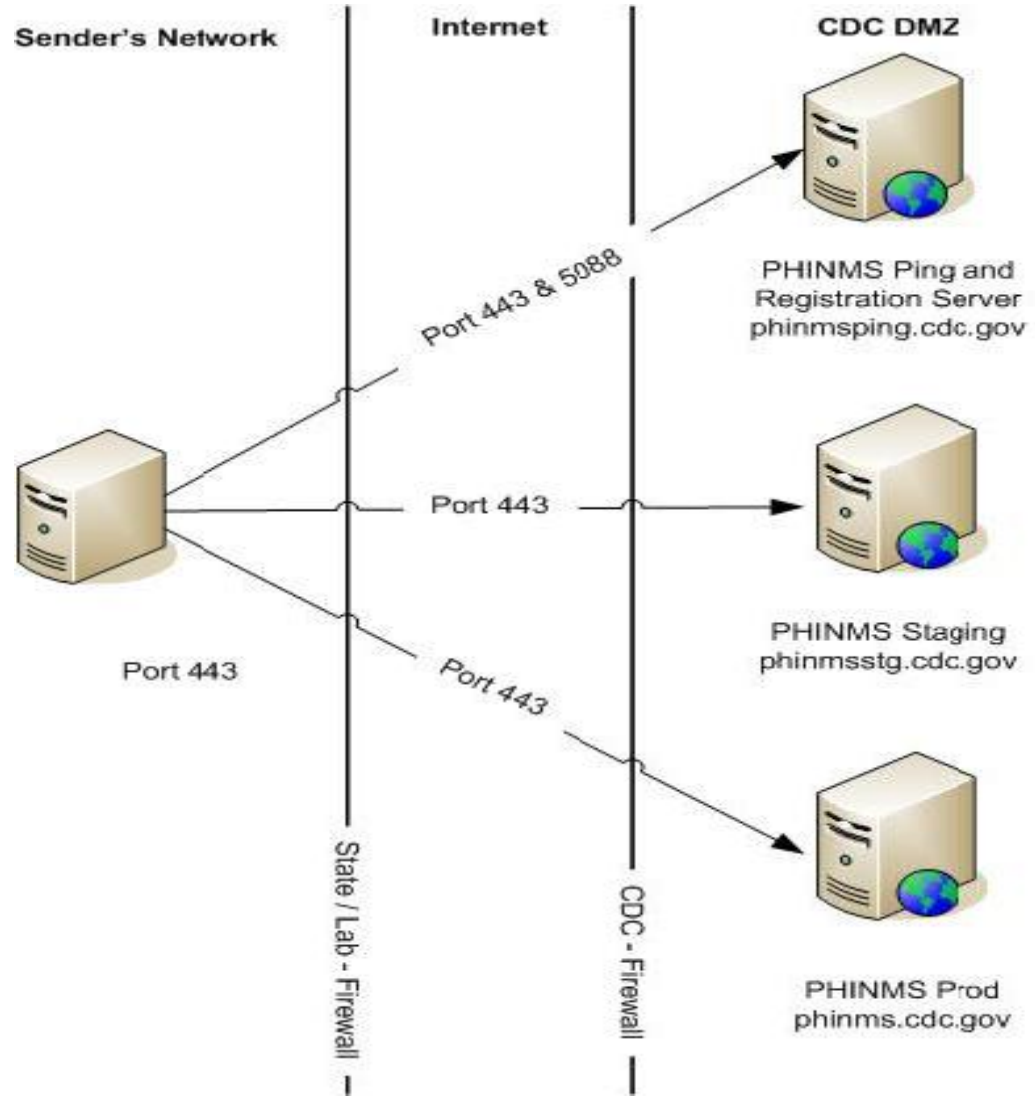


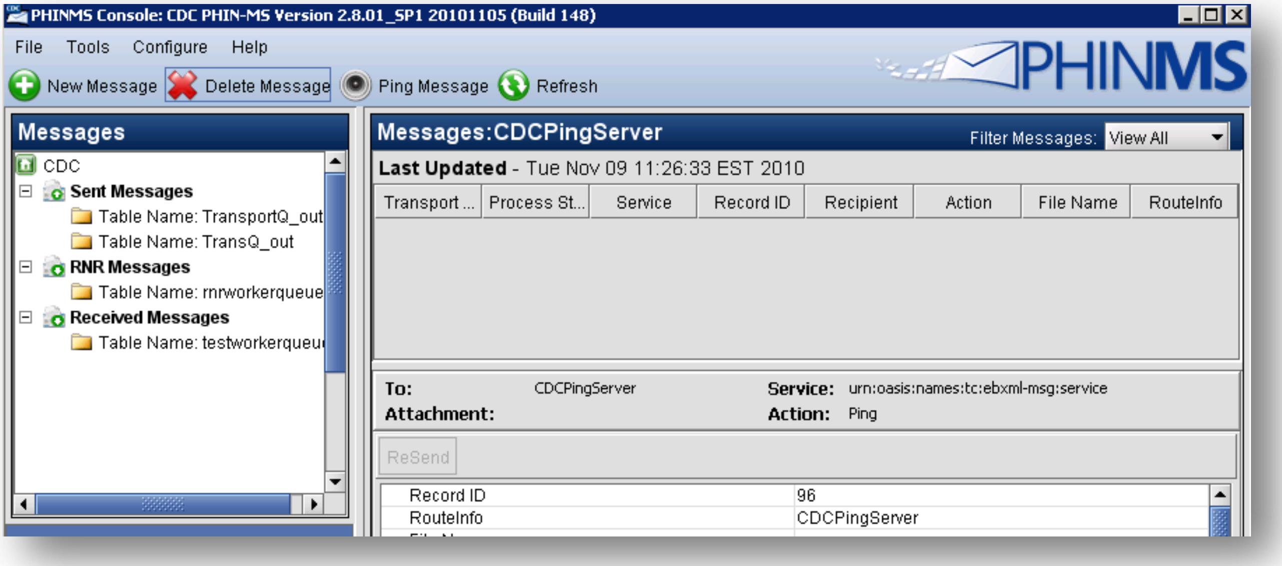
Figure 6.1. CDC PHINMS Topology

6.1 Ping Loopback

The Ping Loopback validates the PHINMS installation was downloaded and installed successfully on the Sender's system. This is not a test to verify messages can be sent outside of a firewall if one is present.

Verify the generated ping loopback is successfully sent to the loopback message processor by completing the following steps:

1. Open the PHINMS 2.8.02 Console displaying Figure 6.2,



Last Updated - Tue Nov 09 11:26:33 EST 2010

Transport ...	Process St...	Service	Record ID	Recipient	Action	File Name	RouteInfo

To: CDCPingServer
Service: urn:oasis:names:tc:ebxml-msg:service
Attachment:
Action: Ping

Record ID	96
RouteInfo	CDCPingServer

Figure 6.2. PHINMS 2.8.02Console

2. Select Ping Message displaying Figure 6.3,

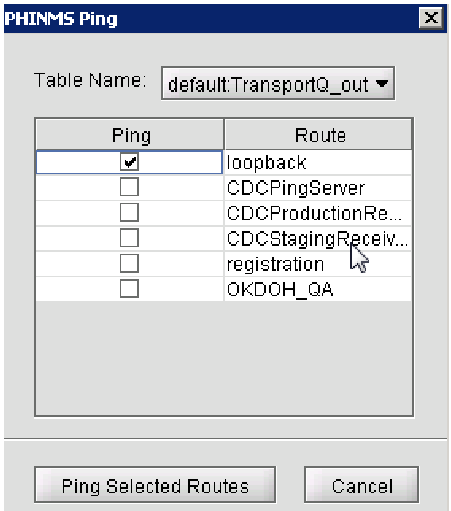
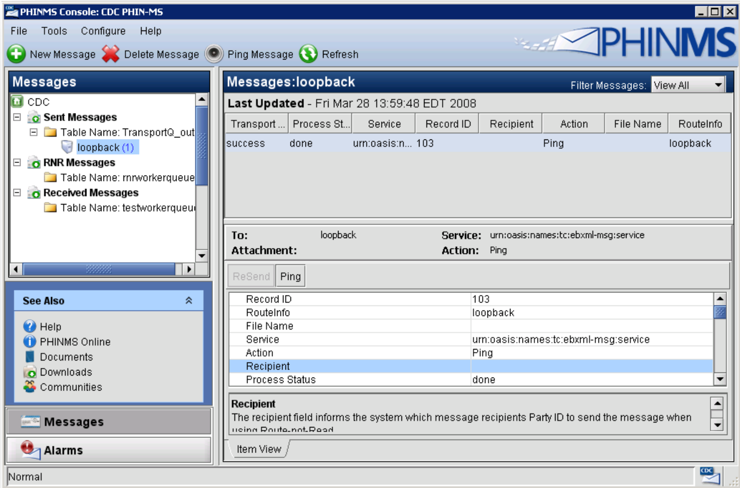


Table Name: default:TransportQ_out

Ping	Route
☑	loopback
☐	CDCPingServer
☐	CDCProductionRe...
☐	CDCStagingReceiv...
☐	registration
☐	OKDOH_QA

Figure 6.3. PHINMS Ping

3. Select loopback,
4. Select Ping Selected Routes displaying Figure 6.4, and



Last Updated - Fri Mar 28 13:59:48 EDT 2008

Transport ...	Process St...	Service	Record ID	Recipient	Action	File Name	RouteInfo
success	done	urn:oasis:n...	103		Ping		loopback

To: loopback **Service:** urn:oasis:names:tc:ebxml-msg:service
Attachment: **Action:** Ping

Record ID	103
RouteInfo	loopback
File Name	
Service	urn:oasis:names:tc:ebxml-msg:service
Action	Ping
Recipient	
Process Status	done

Recipient
The recipient field informs the system which message recipients Party ID to send the message when using Route-not-Read

Figure 6.4. Ping Message

5. Select the loopback folder showing the status of the ping on the right-hand side.

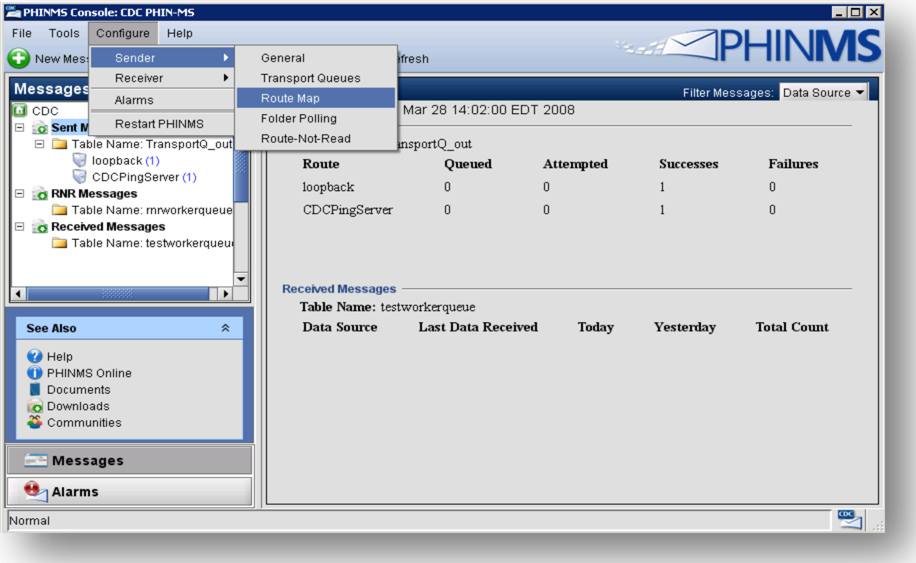
Note: When the Transport Status is in the state of queued or attempted, select Refresh until the status changes.

6.2 Configure CDC Staging Receiver Route Map

Note: Perform these steps only if sending to the CDC. A digital certificate must be obtained for Program TEST, activity PHINMS 2.0 via https://ca.cdc.gov before a successful ping test can be sent.

The CDC Staging Receiver requires to be configured before sending a Ping. Configure the CDCStagingReceiver using the following steps:

1. Open the PHINMS 2.8.02Console displaying Figure 6.5,



Mar 28 14:02:00 EDT 2008

nsportQ_out

Route	Queued	Attempted	Successes	Failures
loopback	0	0	1	0
CDCPingServer	0	0	1	0

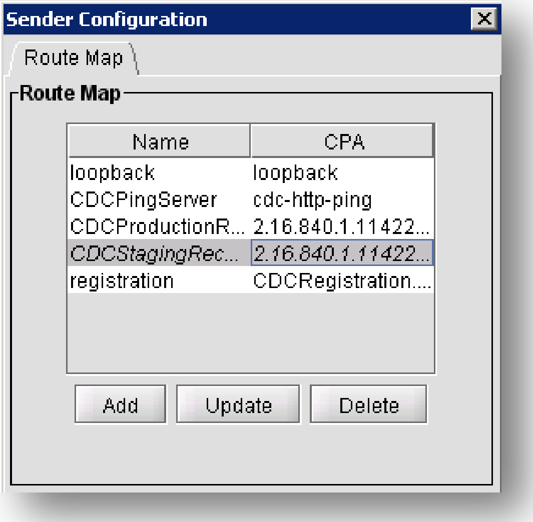
Received Messages

Table Name: testworkerqueue

Data Source	Last Data Received	Today	Yesterday	Total Count

Figure 6.5. PHINMS 2.8.02Console

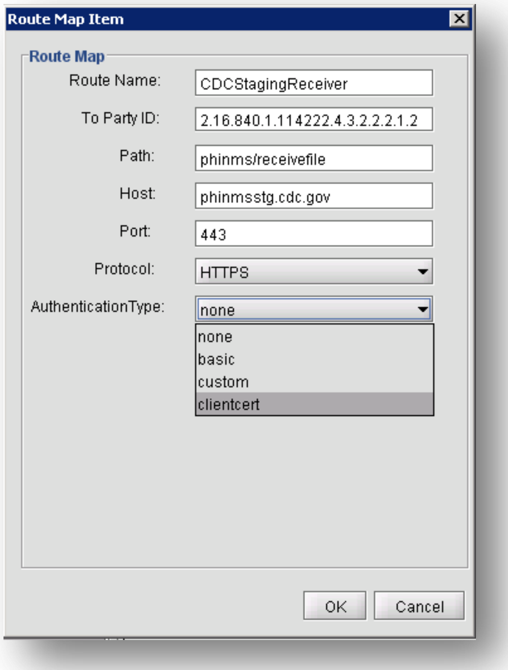
2. Open the select Configure>Sender>Route Map displaying Figure 6.5,



Name	CPA
loopback	loopback
CDCPingServer	cdc-http-ping
CDCProductionR...	2.16.840.1.11422...
CDCStagingRec...	2.16.840.1.11422...
registration	CDCRegistration....

Figure 6.6. Sender Configuration

3. Select CDCStagingReceiver,
4. Select Update displaying Figure 6.6,



Route Map Item

Route Map

Route Name: CDCStagingReceiver

To Party ID: 2.16.840.1.114222.4.3.2.2.2.1.2

Path: phinms/receivefile

Host: phinmsstg.cdc.gov

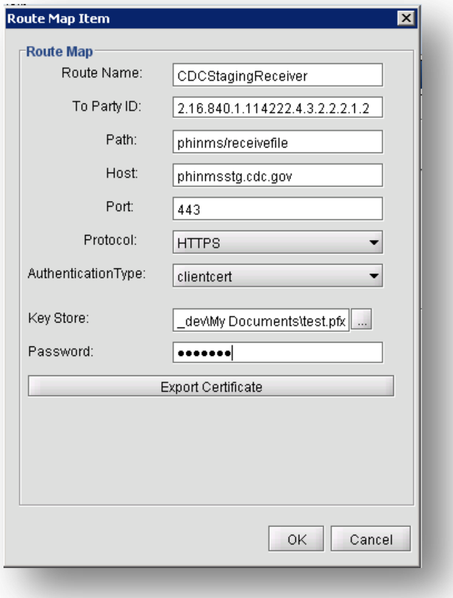
Port: 443

Protocol: HTTPS

AuthenticationType: none

Figure 6.7. Route Map Item

5. Select “clientcert” from the Authentication Type dropdown list displaying Figure 6.7,



Route Map Item

Route Map

Route Name: CDCStagingReceiver

To Party ID: 2.16.840.1.114222.4.3.2.2.2.1.2

Path: phinms/receivefile

Host: phinmsstg.cdc.gov

Port: 443

Protocol: HTTPS

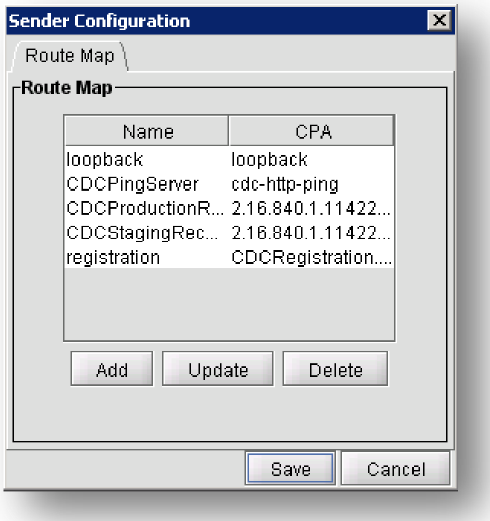
AuthenticationType: clientcert

Key Store: _dev\My Documents\test.pfx

Password: •••••••

Figure 6.8. CDC Route Map Configuration

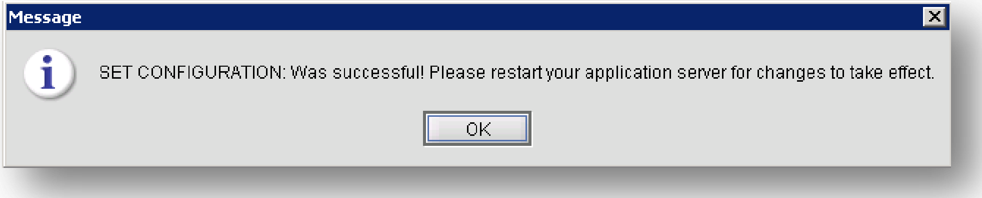
6. Enter the path to the stored certificate Key Store (.pfx or .p12 file), this is the digital certificate issued to the person who applied for an Secure Data Network (SDN).
7. Enter the Key Store Password in the Key Store Password field,
8. Select OK, displaying Figure 6.8,



Name	CPA
loopback	loopback
CDCPingServer	cdc-http-ping
CDCProductionR...	2.16.840.1.11422...
CDCStagingRec...	2.16.840.1.11422...
registration	CDCRegistration....

Figure 6.9. CDC Route Map

9. Select Save, displaying Figure 6.9,



SET CONFIGURATION: Was successful! Please restart your application server for changes to take effect.

Figure 6.10. CDC Route Configuration Successful

10. Select OK, and
11. Restart PHINMS.
12. Go to the PHINMS Console menu select Configure and Restart PHINMS, displaying in Figure 6.11

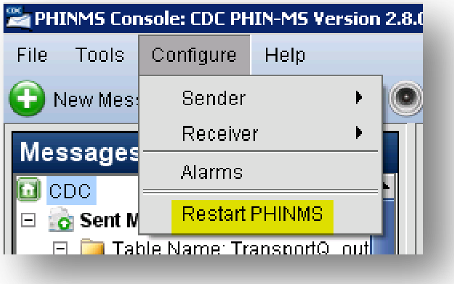


Figure 6.11. Restart PHINMS Console

6.3 Ping a Valid PHINMS Route

The Ping Message validates the Sender can connect to the internet and to the selected route Verify the PING Message to the selected route is successful by completing the following steps:

1. Open the PHINMS 2.8.02 Console displaying,

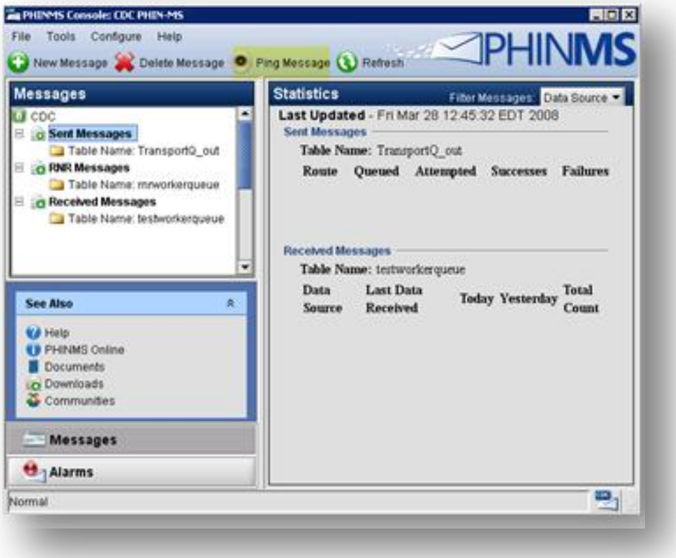


Figure 6.12. PHINMS 2.8.02Console

2. Select Ping Message displaying Figure 6.12,

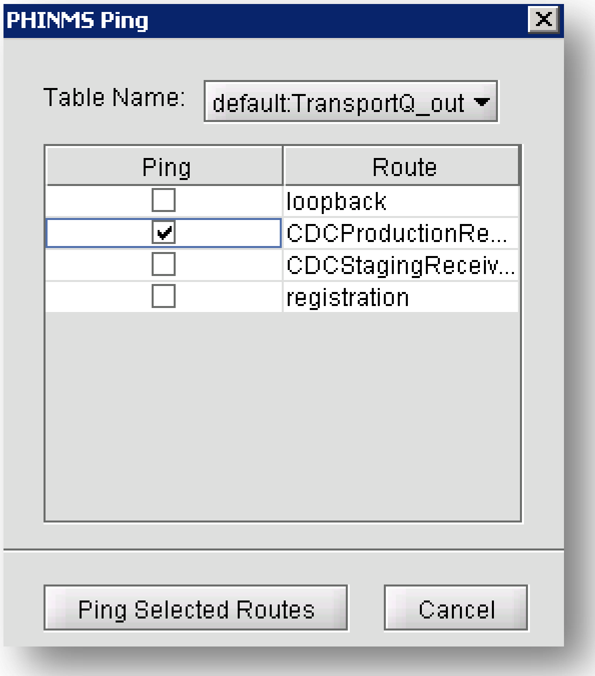


Table Name: default:TransportQ_out

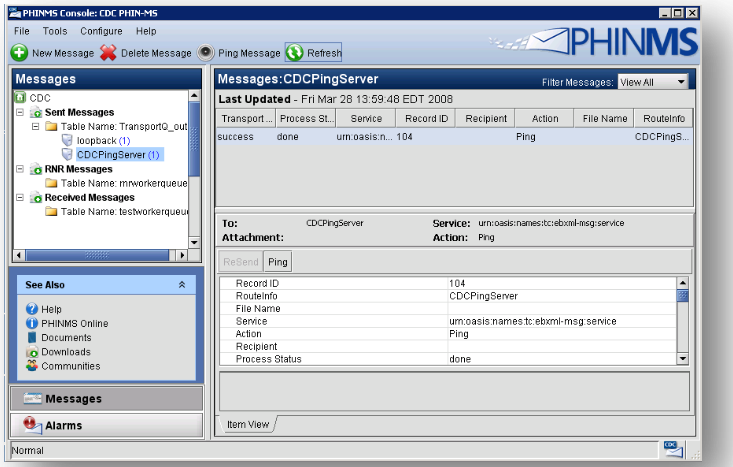
Ping	Route
□	loopback
☑	CDCProductionRe...
□	CDCStagingReceiv...
□	registration

Figure 6.13. PHINMS Ping

3. Select route of choice, (example shows CDCStagingReceiver).

Note: You must have a valid digital certificate configured to ping any route requiring client certificate authentication.

4. Select Ping Selected Routes displaying Figure 6.13, and



Messages:CDCPingServer

Last Updated - Fri Mar 28 13:59:48 EDT 2008

Transport ...	Process St...	Service	Record ID	Recipient	Action	File Name	RouteInfo
success	done	urn:oasis:n...	104		Ping		CDCPingS...

To: CDCPingServer **Service:** urn:oasis:names:tc:ebxml-msg:service

Attachment: **Action:** Ping

Record ID	104
RouteInfo	CDCPingServer
File Name	
Service	urn:oasis:names:tc:ebxml-msg:service
Action	Ping
Recipient	
Process Status	done

Figure 6.14. Ping Message

5. Select the Route's folder showing the status of the ping on the right-hand side.

Note: When the Transport Status is in the state of queued or attempted, select Refresh until the status changes.

6.4 Email CPA File

PHINMS creates a Collaboration Protocol Agreement (CPA) file for each route listed in the PHINMS Route Map tab of the Sender Configuration panel. The PHINMS Administrator must export the CPA for any route configured and send the related CPA to the receiving site to import into the receiving PHINMS console. To send to the CDC, export and send the PHINMS Helpdesk (Phintech@cdc.gov) the CPA files for the CDC Production Receiver or the CDC Staging Receiver. Only after the PHIN helpdesk has received the CPA file and applied it to the PHINMS Receiver can there be a successful transmission of messages from the Sender to the Receiver.

The CPA files required to be sent are located in directory C :\(PHINMS install directory)\ config\sender \CPA.

Note: Information on CPA can be found in the PHINMS Technical Reference Guide.

6.5 Export the CPA file

1. Open the PHINMS Console and select the Tools option, displaying in Figure 6.15

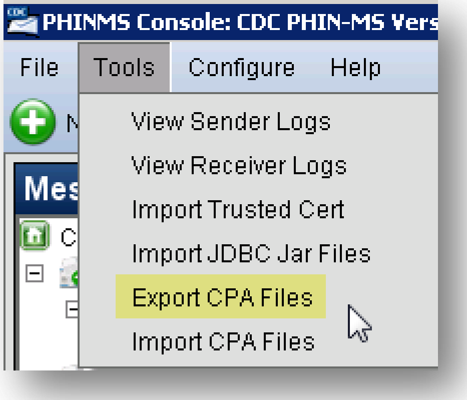
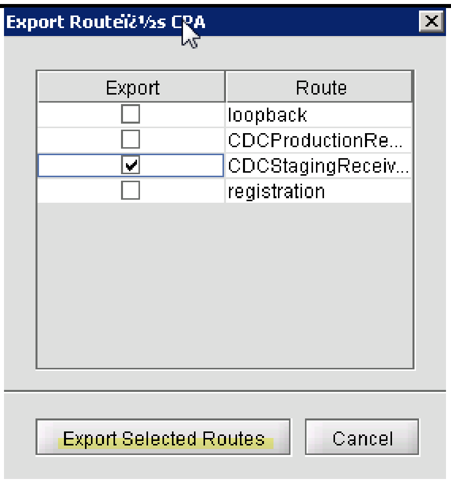


Figure 6.15 PHINMS Tools Option

2. Select Export CPA Files
3. Select the route to export CPA, displaying in Figure 6.16 below (ex: CDCStagingReceiver route),



Export Routeï¿½s CPA

Export	Route
□	loopback
□	CDCProductionRe...
☑	CDCStagingReceiv...
□	registration

Figure 6.16. Export Route CPA

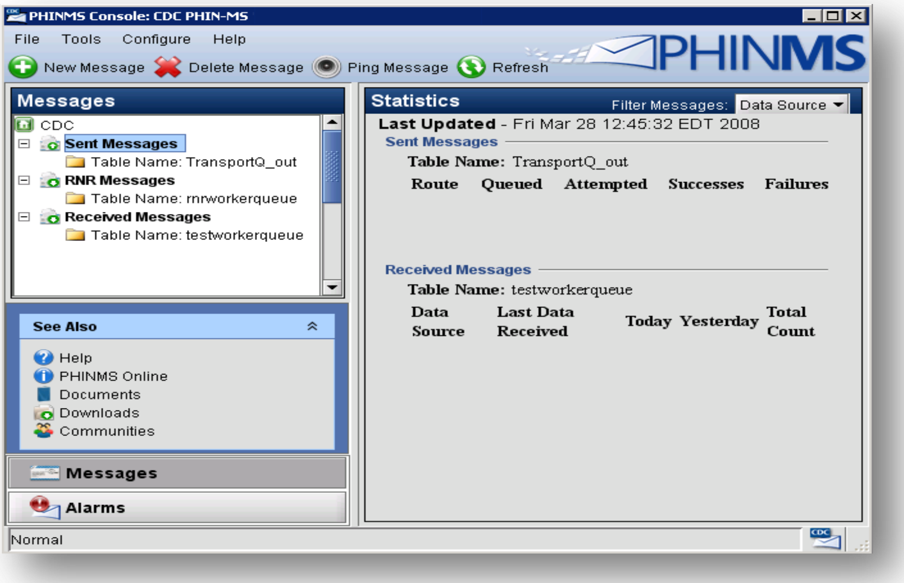
4. Select Export Selected Routes, displaying in Figure 6.16 above
5. Select Open after browsing to the location where the CPA file will be exported.
6. Email the CPA xml file to the appropriate receiving site.
7. Once the receiving site has confirmed the CPA file is imported, the following steps can be perfomed to test the route.

6.6 Send Test Payload Message

The send payload message verifies the capability to send an outbound message with an attached file to a Receiver. Ensure the CPA files have been sent to the PHIN Help desk before attempting to send a payload message to the CDC. Refer to Section 9.1 for CPA information.

Send the payload message test to the PHINMS Staging Receiver by completing the following steps:

1. Open the PHINMS 2.8.02 Console displaying Figure 6.17,



Messages

- CDC
  - Sent Messages
    - Table Name: TransportQ_out
  - RNR Messages
    - Table Name: rnrworkerqueue
  - Received Messages
    - Table Name: testworkerqueue

Statistics — Filter Messages: Data Source

Last Updated - Fri Mar 28 12:45:32 EDT 2008

Sent Messages

Table Name: TransportQ_out

Route	Queued	Attempted	Successes	Failures

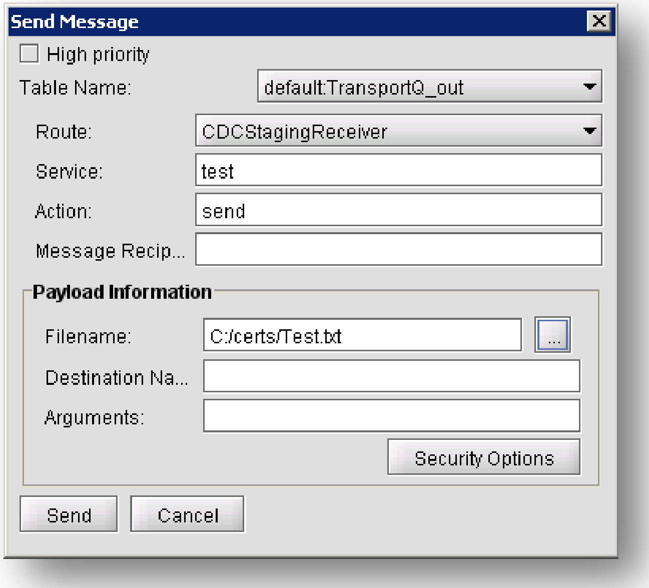
Received Messages

Table Name: testworkerqueue

Data Source	Last Data Received	Today	Yesterday	Total Count

Figure 6.17. PHINMS 2.8.02Console

2. Select New Message from the console displaying Figure 6.18,



Send Message

☐ High priority

Table Name:	default:TransportQ_out
Route:	CDCStagingReceiver
Service:	test
Action:	send
Message Recip...	

Payload Information

Filename:	C:/certs/Test.txt
Destination Na...	
Arguments:	

Figure 6.18. PHINMS Ping

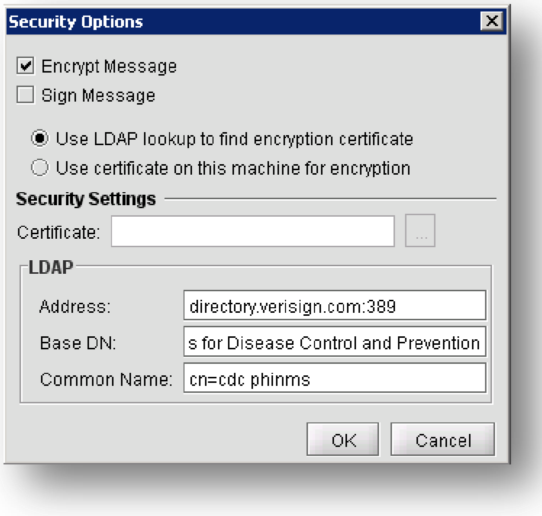
3. Enter the following parameters provided by the receiving site or if sending to CDCStaging use the parameters below:
   - **Route:** CDC Staging Receiver,

- **Service:** test,
- **Action:** send,
- **Message Recipient:** optional - can be left blank,
- **Filename:** browse for a file to attach,
- **Destination Name:** optional - can be left blank,
- **Arguments:** optional - can be left blank,

4. Proceed to Step 5 if using Security Options and to Step 8 if not,

Note: Security Options are optional for encrypting or signing messages.

5. Select Security Options displaying Figure 6.19,



Security Options

☑ Encrypt Message

☐ Sign Message

● Use LDAP lookup to find encryption certificate

○ Use certificate on this machine for encryption

Security Settings

Certificate:

LDAP

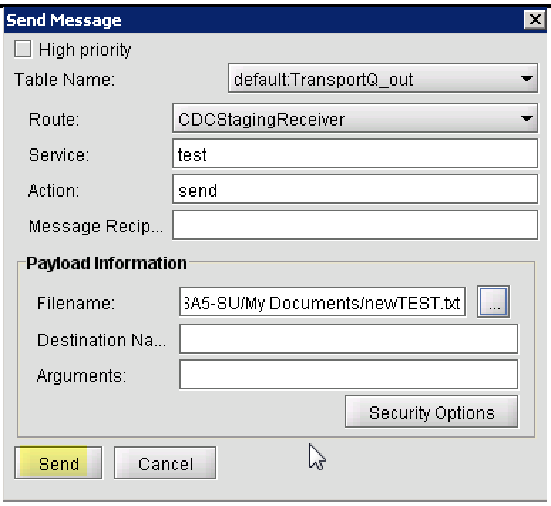
Address: directory.verisign.com:389

Base DN: s for Disease Control and Prevention

Common Name: cn=cdc phinms

Figure 6.19. Security Options

6. Enter the following parameters:
   - **check Encrypt Message,**
   - **select Use LDAP lookup to find encryption certificate,**
   - **Address: directory.verisign.com:389,**
   - **BaseDN: o=Centers for Disease Control and Prevention,**
   - **Common Name: cn=cdc phinms,**
7. Select OK,
8. Select Send displaying Figure 6.20,



Send Message

□ High priority

Table Name: default:TransportQ_out

Route: CDCStagingReceiver

Service: test

Action: send

Message Recip...

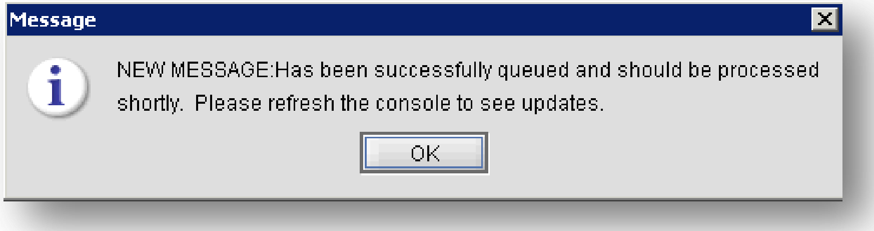
Payload Information

Filename: 3A5-SU/My Documents/newTEST.txt

Destination Na...

Arguments:

Figure 6.20 Send Message



Message

NEW MESSAGE:Has been successfully queued and should be processed shortly. Please refresh the console to see updates.

Figure 6.21. New Message Notification

8. Select OK, Figure 6.21

7.0 RECEIVER INFORMATION

7.1 Configure WorkerQ

The Worker Queue (WorkerQ) is the database table used for storing inbound messages. When configured from the Receiver configuration screen in the Console, it is used to drop incoming messages sent to the Receiver. The database configuration needs to be completed before creating WorkerQ table. The instructions to configure a database connection to the external database are in Section 5.0.

If configured from the Sender configuration screen in the Console, it is used to write the responses to polling requests (route-not-read configuration). More information on Sender configuration can be located in the PHINMS Technical Reference Guide.

Create an external database WorkerQ table by following steps below:

1. Open the PHINMS 2.8.02 Console displaying Figure 7.1,

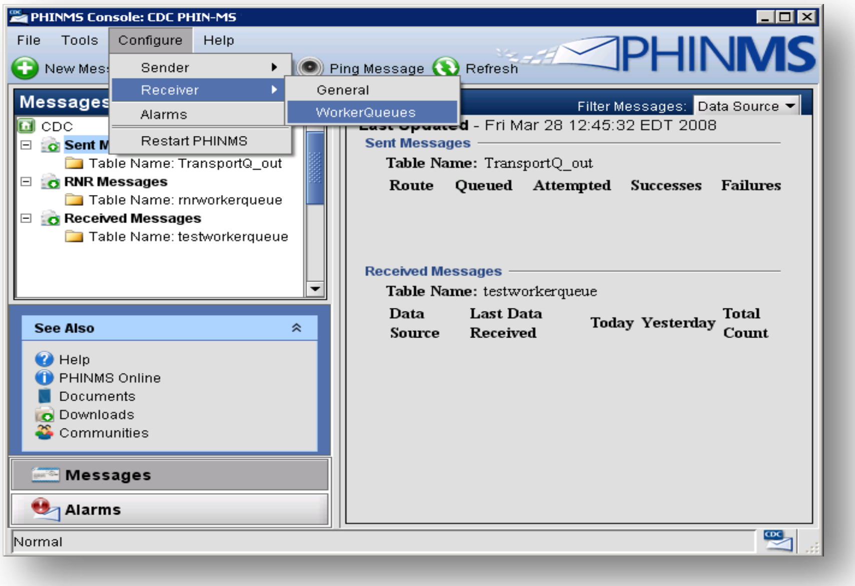
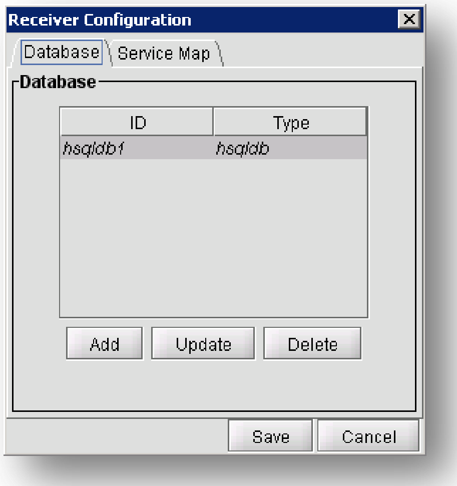


Figure 7.1. PHINMS 2.8.02Console

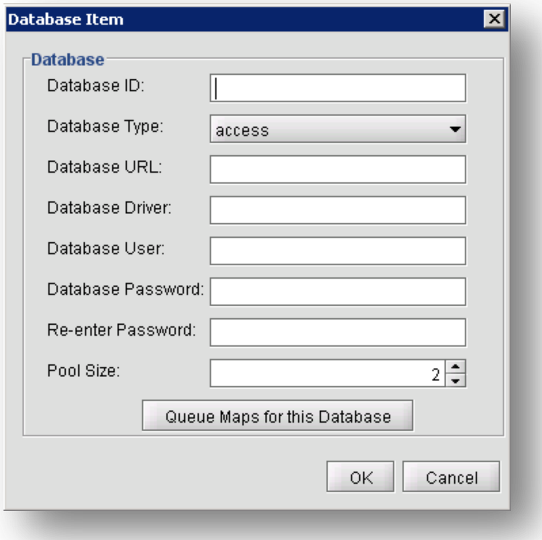
2. Select Configure>Receiver>WorkerQueues displaying Figure 7.2,



ID	Type
hsqldb1	*hsqldb*

Figure 7.2. Receiver Configuration - Database

3. Select Add displaying Figure 7.3,



Database ID:	
Database Type:	access
Database URL:	
Database Driver:	
Database User:	
Database Password:	
Re-enter Password:	
Pool Size:	2

Figure 7.3. Database Item

4. Enter the database items, displaying in Figure 7.4. Refer to Table 4 for an explanation of the values,

TAG VALUE	DESCRIPTION
Database ID	The unique name for the database connection pool, referenced in the queue map. The service map uses the **databaseId** to map the queue to a specific database. (The unique databaseId is determined by the user.)

TAG VALUE	DESCRIPTION
Database Type	Designates the type of database.
Database URL	The URL to the database. The URL depends on the type of database and driver used such as **jdbc:sqlserver://host:portnumber;DatabaseName=database** for Microsoft SQL Server and **jdbc:oracle://host:port:sid** for Oracle.
Database Driver	The type of JDBC driver. The JDBC driver should be appropriate for the type of database such as **com.microsoft.sqlserver.jdbc.SQLServerDriver** for Microsoft SQL Server and **oracle.jdbc.OracleDriver** for Oracle.
Database User	This user account is provided by the database administrator for login purposes which is used to automate the login process via PHINMS. A pointer to the database user entry in the Message Receiver's encrypted password store. The value is not the database user but the name of the tag within the password file. The value of the tag contains the actual database user name.
Database Password	This password is provided as part of the user account created by the database administrator for login purposes which is used to automate the login process via PHINMS.A pointer to the database password entry in the Message Receiver's encrypted password store. The value is not the database password but the tag within the password file. The value of the tag contains the actual database password.
Pool Size	The number of database connections to open. When setting the pool size ensure the system can handle the maximum client load while keeping enough memory available.

Table 4. WorkerQ Database Tag Values

5. Select Queue maps for this Database displaying Figure 7.4,

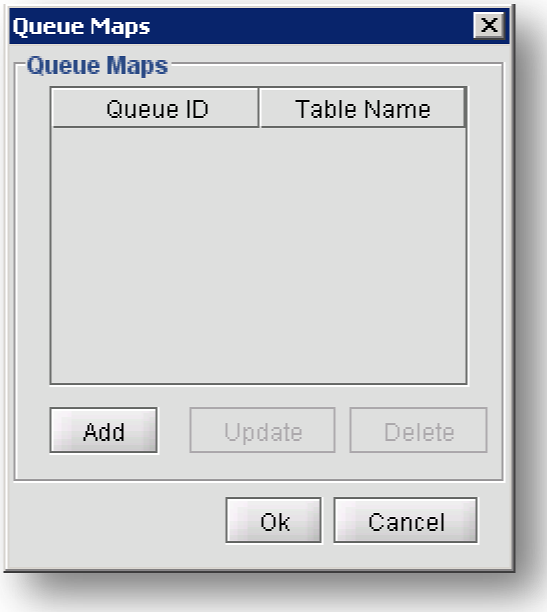


Figure 7.4. Queue Maps

6. Select Add displaying Figure 7.5,

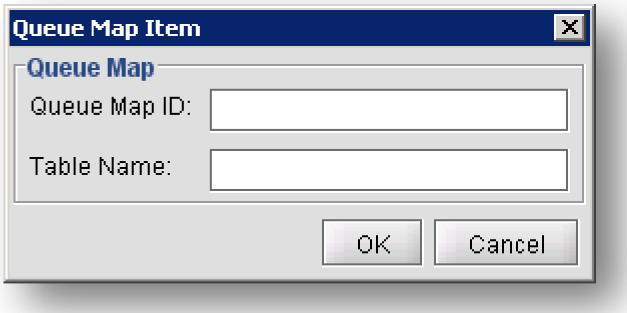
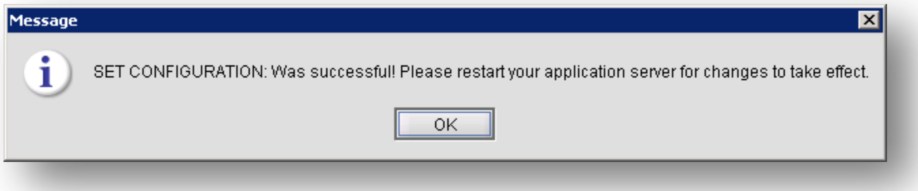


Figure 7.5. Queue Map Item

7. Enter Queue Map ID, (The Queue Map ID is determined by the user.)
8. Enter Table Name,
   - » Click OK,
   - » Click OK,
   - » Click OK,
9. Click Save,



SET CONFIGURATION: Was successful! Please restart your application server for changes to take effect.

Figure 7.6. WorkerQ Database Configuration Successful

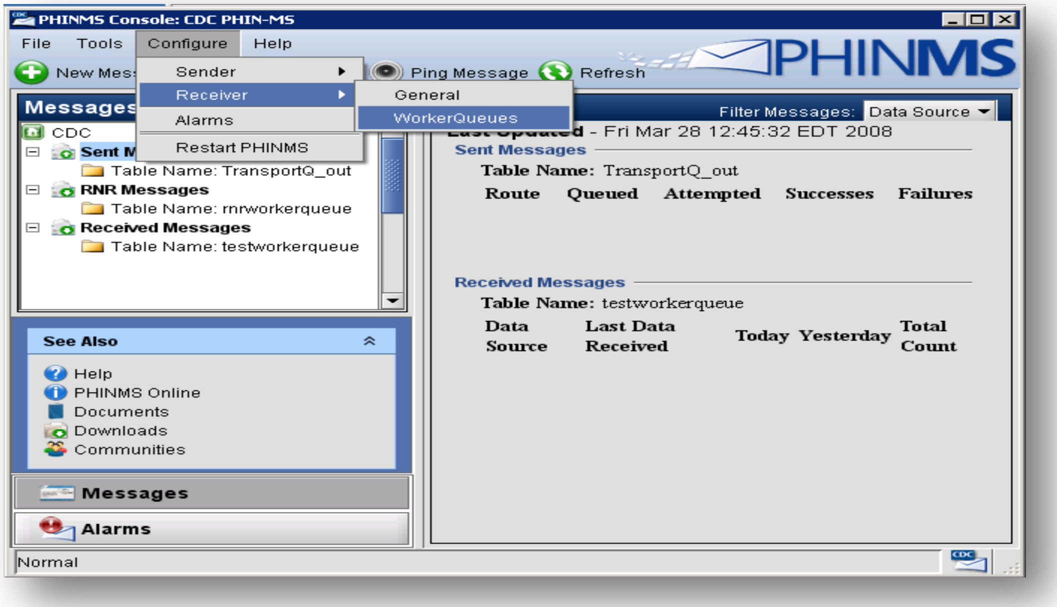
10. Select OK,
11. From the console menu select Configure, Restart PHINMS.

7.2 Create Service and Action Pair

PHINMS 2.8.02 uses message envelopes for each sent message. The envelope has addressing information tags called Service and Action known as character strings. Character strings are logically mapped to an application queue on the receiving side. The Service and Action tags determine the message type.

Create a Service and Action pair by completing the following steps:

1. Open the PHINMS 2.8.02Console displaying Figure 7.7,



CDC
- Sent M
  - Table Name: TransportQ_out
- RNR Messages
  - Table Name: rnrworkerqueue
- Received Messages
  - Table Name: testworkerqueue

Last Updated - Fri Mar 28 12:45:32 EDT 2008

Sent Messages

Table Name: TransportQ_out

Route	Queued	Attempted	Successes	Failures

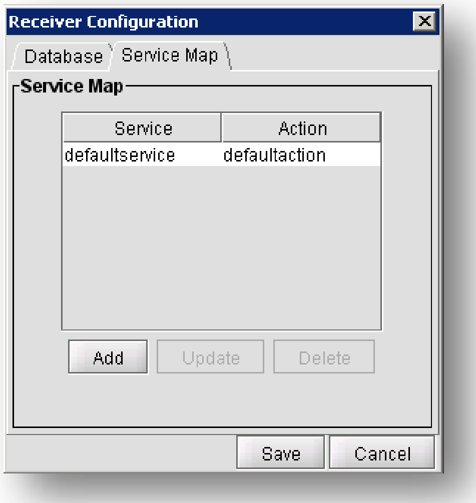
Received Messages

Table Name: testworkerqueue

Data Source	Last Data Received	Today	Yesterday	Total Count

Figure 7.7. PHINMS 2.8.02Console

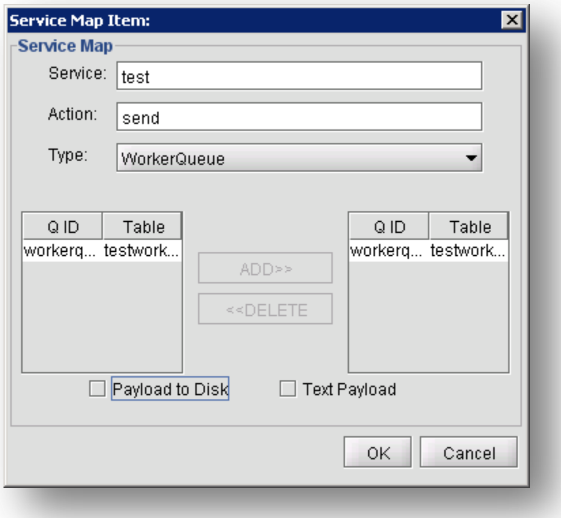
2. Select Configure>Receiver>WorkerQueues displaying Figure 7.8,



Service	Action
defaultservice	defaultaction

Figure 7.8. Service Map

3. Select Service Map,
4. Select Add displaying Figure 7.9,



Service: test

Action: send

Type: WorkerQueue

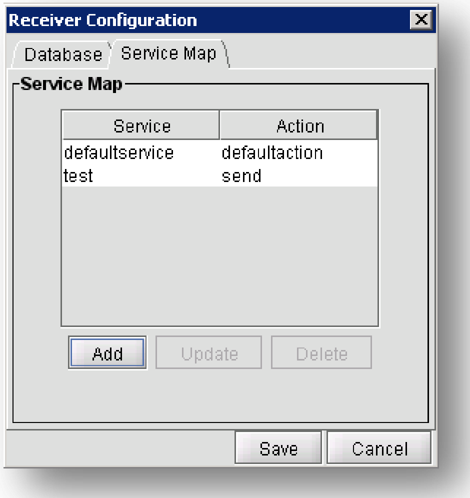
Q ID	Table
workerq...	testwork...

Q ID	Table
workerq...	testwork...

□ Payload to Disk □ Text Payload

Figure 7.9. Service Map Item

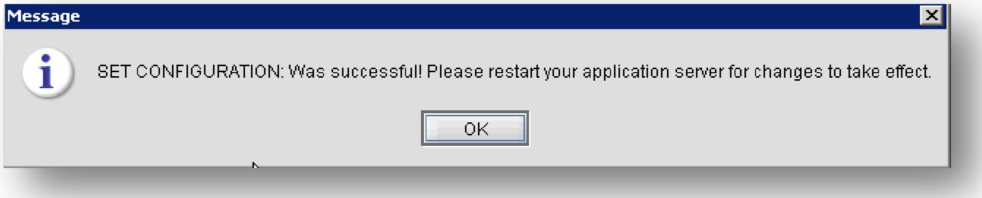
5. Enter Service,
6. Enter Action,
7. Select WorkerQueue from the dropdown list,
8. Highlight workerqueue located under Q ID on the left-hand side,
9. Select Add,
10. Select OK displaying Figure 7.10,



Service	Action
defaultservice	defaultaction
test	send

Figure 7.10. Service and Action Added

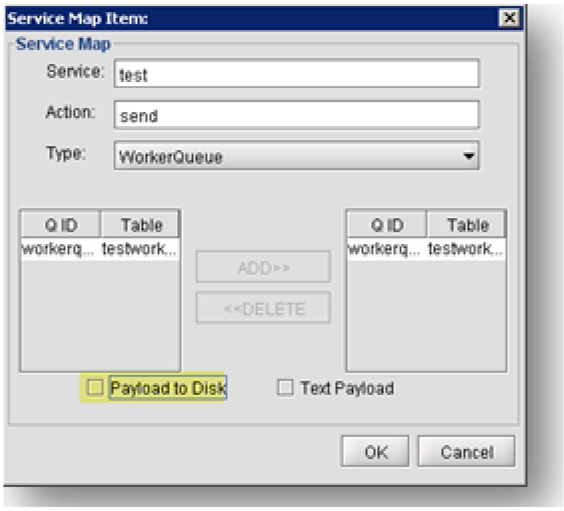
11. Select Save displaying Figure 7.11,



SET CONFIGURATION: Was successful! Please restart your application server for changes to take effect.

Figure 7.11. Service and Action Successful Configuration

12. Click OK, and
13. Restart PHINMS.



Service: test

Action: send

Type: WorkerQueue

Q ID	Table
workerq...	testwork...

Q ID	Table
workerq...	testwork...

□ Payload to Disk □ Text Payload

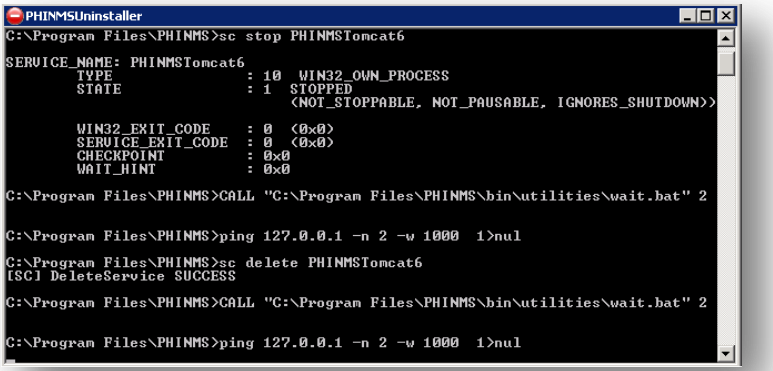
Figure 7.12. Service Map Item

Note: When Payload to Disk is checked, display3e in Figure 7.12, the incoming payload is written to disk instead of to the database field. The default location for payload to disk is (ex: *C:\Program Files\PHINMS\shared\receiverincoming*

8.0 UNINSTALL PHINMS 2.8.02

Complete the following steps to uninstall PHINMS 2.8.02:

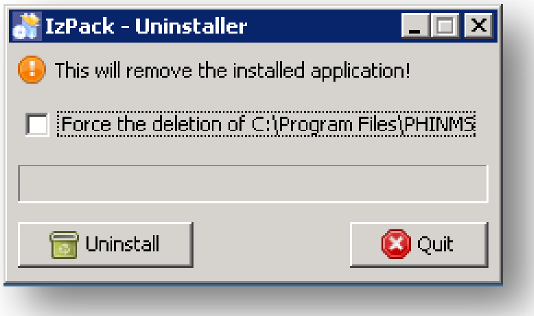
1. Select Start>Programs>PHINMS>Uninstall PHINMS displaying Figure 8.1,



```
C:\Program Files\PHINMS>sc stop PHINMSTomcat6

SERVICE_NAME: PHINMSTomcat6
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
                               (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN))

        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\Program Files\PHINMS>CALL "C:\Program Files\PHINMS\bin\utilities\wait.bat" 2


C:\Program Files\PHINMS>ping 127.0.0.1 -n 2 -w 1000  1>nul

C:\Program Files\PHINMS>sc delete PHINMSTomcat6
[SC] DeleteService SUCCESS

C:\Program Files\PHINMS>CALL "C:\Program Files\PHINMS\bin\utilities\wait.bat" 2


C:\Program Files\PHINMS>ping 127.0.0.1 -n 2 -w 1000  1>nul
```

Figure 8.1. PHINMS Uninstaller screen

2. The DOS window displays the services are stopped and deleted at which time the application uninstaller screen is initiated displaying Figure 8.2,

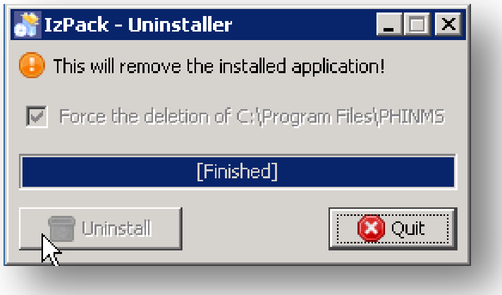


This will remove the installed application!

□ Force the deletion of C:\Program Files\PHINMS

Figure 8.2. Application Uninstaller

3. Select “Force the deletion of the PHINMS install directory folder structure” then click Uninstall displaying Figure 8.3, and



IzPack - Uninstaller

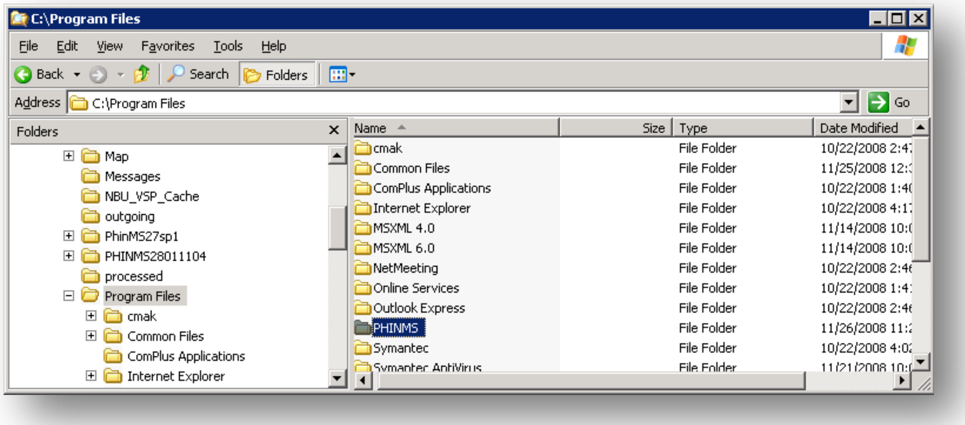
This will remove the installed application!

☑ Force the deletion of C:\Program Files\PHINMS

[Finished]

Figure 8.3. Successful Uninstall

4. Click Quit.
5. Navigate to the PHINMS install directory displaying Figure 8.4,



C:\Program Files

Address C:\Program Files

Folders:
- Map
- Messages
- NBU_VSP_Cache
- outgoing
- PhinMS27sp1
- PHINMS28011104
- processed
- Program Files
  - cmak
  - Common Files
  - ComPlus Applications
  - Internet Explorer

Name	Size	Type	Date Modified
cmak		File Folder	10/22/2008 2:4
Common Files		File Folder	11/25/2008 12:
ComPlus Applications		File Folder	10/22/2008 1:4
Internet Explorer		File Folder	10/22/2008 4:1
MSXML 4.0		File Folder	11/14/2008 10:
MSXML 6.0		File Folder	11/14/2008 10:
NetMeeting		File Folder	10/22/2008 2:4
Online Services		File Folder	10/22/2008 1:4
Outlook Express		File Folder	10/22/2008 2:4
PHINMS		File Folder	11/26/2008 11:
Symantec		File Folder	10/22/2008 4:0
Symantec AntiVirus		File Folder	11/21/2008 10:

Figure 8.4. PHINMS install directory

6. Delete the PHINMS install directory. You have successfully uninstalled PHINMS 2.8.02.

9.0 ADDITIONAL FEATURES

9.1 Import CPA

PHINMS 2.8.02allows the user to import the CPA directly from the PHINMS 2.8.02Console. Complete the following steps to import the CPA:

1. Open the PHINMS 2.8.02 Console,
2. Select Tools,
3. Select Import CPA,
4. Select the CPA to import,
5. Select Open, and
6. Select OK.

9.2 View Receiver Logs

The Receiver Logs stores information on the status of received messages and can be viewed directly from the PHINMS 2.8.02Console. Viewing the logs allows users to check the status of received messages. Complete the following steps to view the Receiver Logs:

1. Open the PHINMS 2.8.02 Console,
2. Select Tools,
3. Select Receiver Logs,
4. Select the Route from the drop-down list,
5. Select Date, and
6. Select View displaying the text.

9.3 View Sender Logs

The Sender Logs stores information on the status of send messages and can be viewed directly from the PHINMS 2.8.02Console. Viewing the logs allows users to check the status of sent messages. Complete the following steps to view the Sender Logs:

1. Open the PHINMS 2.8.02Console,
2. Select Tools,
3. Select View Sender Logs,
4. Select Route from the drop-down list,
5. Select Date, and
6. Select View displaying the text.

9.4 Import Trusted Certificate

A Trusted Certificate consists of a root and intermediate CA certificate. When the browser is trying to make an SSL connection, it needs to validate the Certificate Chain of the SSL certificate installed on the proxy server on the Receiver’s end. PHINMS Sender verifies the Chain using CACERTS Key Store file. If the Chain does not match, the Sender has to import the Trusted Certificate into the CACERTS Key Store file by using an import option

The user can now import the Trusted Certificate directly from the PHINMS 2.8.02Console. Complete the following steps to import the Trusted Certificate:

1. Open the PHINMS 2.8.02Console,
2. Select Tools,
3. Select Import Trusted Cert,
4. Navigate to the location the Trusted Certificate is stored,
5. Select the Trusted Certificate (.cer or .pem file) to import, and
6. Select Open, successfully importing the Trusted Certificate into the Sender's trusted CA certificate store.

9.5 Import JDBC JAR Files

JDBC Jar Files are able to be imported directly from the PHINMS 2.8.02Console. Complete the following steps to import the three (3) JDBC Jar Files:

1. Open the PHINMS 2.8.02Console,
2. Select Tools,
3. Select Import JDBC Jar Files,
4. Locate and select the jdbc driver for your database (see Table 1. JDBC Drivers, section 2.1, page 11 for recommended jdbc drivers)
5. Select Open,
6. A message will indicate a successful import, select OK, and
7. Restart PHINMS Tomcat Instance located in the Windows services console.

9.6 Change Login Password

PHINMS 2.8.02allows the user to change the Console login password. Complete the following steps to successfully change the login password:

1. Open the PHINMS 2.8.02Console,
2. Select File,
3. Select Change Login Password,
4. Enter the Old Console Password,
5. Enter the New Console Password and Re-Enter New Console Password,
6. Select Change Password,
7. Click OK, and
8. Restart PHINMS 2.8 Apache Tomcat service.

9.7 Sender and Receiver Alarms

PHINMS 2.8.02contains system alarms for the Sender and Receiver. This feature allows the user to acknowledge and enter a resolution for each alarm. Configure the alarm features by completing the following steps:

1. Open the PHINMS 2.8.02Console,

2. Select Configure, Alarms,
3. Check Report Alarms

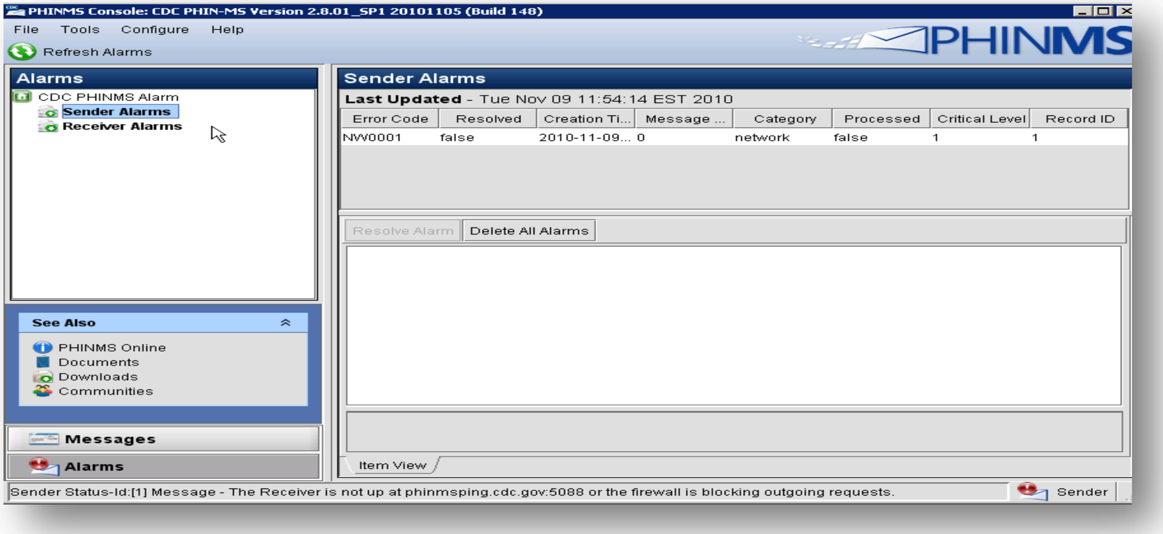
Note: When the Report Alarms is selected, the alarms can be viewed in the Console and enabling the configuration of the Email Alarms feature.

4. Complete the following fields:
   - » SMTP Server - required,
   - » User Name,
   - » User Password,
   - » Re Enter User Password,
   - » From Address - required,
5. Select OK.

9.8 Alarm Resolution

The Alarm Resolution feature allows the user to view error and help messages. It also allows the user to store the resolution information. Take advantage of the Alarm Resolution feature by completing the following steps:

1. Open the PHINMS 2.8.02 Console, Select Alarms located at the lower left-hand side of the console displaying Figure 9.1,



PHINMS Console: CDC PHIN-MS Version 2.8.01_SP1 20101105 (Build 148)

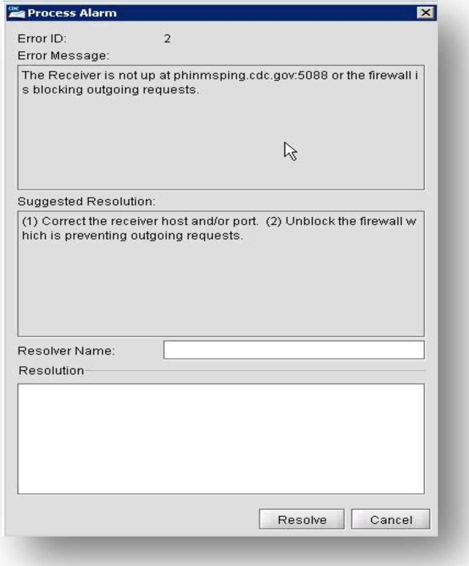
Last Updated - Tue Nov 09 11:54:14 EST 2010

Error Code	Resolved	Creation Ti...	Message ...	Category	Processed	Critical Level	Record ID
NW0001	false	2010-11-09...	0	network	false	1	1

Sender Status-Id:[1] Message - The Receiver is not up at phinmsping.cdc.gov:5088 or the firewall is blocking outgoing requests.

Figure 9.1. Alarms

2. Select the Message to review,
3. Select Resolve Alarms displaying Figure 9.2,
4. The new release also has the ability to Delete All Alarms,



Error ID: 2

Error Message:

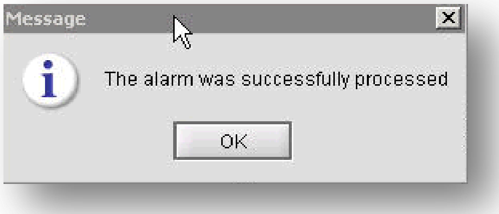
The Receiver is not up at phinmsping.cdc.gov:5088 or the firewall i s blocking outgoing requests.

Suggested Resolution:

(1) Correct the receiver host and/or port. (2) Unblock the firewall w hich is preventing outgoing requests.

Figure 9.2. Alarm Resolution

5. Review the Error Message and the Suggested Resolution,
6. Enter the Resolver Name,
7. Enter the Resolution,
8. Select Resolve displaying Figure 9.3, and



The alarm was successfully processed

Figure 9.3. Alarm Successfully Processed

9. Select OK.

9.9 Folder-Based Polling

This feature makes it much easier for applications to interface with PHINMS 2.8.02. Senders can now configure the Console for Folder-Based Polling. Folder Based Polling allows the Sender to store the messages in a folder and the system will send the messages from the folder instead of a database. The associated route is defined in the Console and does not need file descriptors. Configure the Folder Based Polling feature by completing the following steps:

1. open the PHINMS 2.8.02 Configure,

2. select Configure>Sender>Folder Polling,
3. check Folder Based Polling,
4. select Add,
5. populate the Folder Properties,
6. select Security Options,
7. select OK,
8. select Save,
9. select OK,
10. select the PHINMS 2.8.02Console Restart button,
11. create the following three (3) folders in any directory:
    - Outgoing - used to store messages to be sent,
    - Processed - regional file which messages have been processed, and
    - Acknowledgement - stores the message receipt from the Receiver.

9.10 Transport Queue Auto Delete

1. Open the PHINMS 2.8.02 Console,
2. Select Configure>Sender>TransportQueues,
3. Select the Transport Queue to be modified,
4. Click update,
5. Click Queues for this database,
6. Select the table to be modified,
7. Click update,
8. Locate the auto delete section,
9. Enable Auto delete,
10. Modify Frequency to your desired setting,
11. Configure a start date and time,
12. Modify Retention Period to your desired setting,
13. Click ok, click ok, click ok, click save,
14. Click ok on the acknowledgement,
15. Click configure, and
16. Click Restart PHINMS.

9.11 Worker Queue Auto Delete

1. Open the PHINMS 2.8.02Configure,
2. Select Configure>Receiver>WorkerQueues,
3. Select the WorkerQueues to be modified,
4. Click update,
5. Click Queues for this database,
6. Select the table to be modified,

7. Click update,
8. Locate the auto delete section,
9. Enable Auto delete,
10. Modify Frequency to your desired setting,
11. Configure a start date and time,
12. Modify Retention Period to your desired setting,
13. Click ok, click ok, click ok, click save,
14. Click ok on the acknowledgement,
15. Click configure, and
16. Click Restart PHINMS.

9.12 Secondary Receiver Decryption Certificate

The new releases of PHINMS contains an option to configure a secondary keystore for decrypting files. This is used when there are two valid certificates on Verisign LDAP. If a sender sends an encrypted file, it is possible the file will be encrypted with a certificate that has not expired.

The primary and secondary keystore locations will allow the receiver to configure both new and old certificates. If a file is received encrypted with the new certificate it will decrypt and if it is encrypted with the old cert, it will still decrypt until the expiration date is reached.

1. Open the PHINMS Console
2. Select Configure>>Receiver>>General
3. Select Security Category
4. In the Primary Keystore location, enter the path to the new decryption key
5. Enter the password for the new decryption key
6. In the Secondary Keystore location, enter the path to the older decryption key
7. Enter the password
8. Enter the date the old decryption key expires. Format should be: yyyy-mm-dd hh:mm:ss
9. Save
10. Restart PHINMS

9.13 Secondary Sender Certificate

The new releases of PHINMS contains an option to configure a secondary keystore for decrypting polled files. This feature is an enhancement for Route not Read pollers. This is used when there are two valid certificates on Verisign LDAP. If a sender sends an encrypted file, it is possible the file will be encrypted with a certificate that has not expired.

The primary and secondary keystore locations will allow the poller to configure both new and old certificates. If a file is sent to the RnR hub encrypted with the new certificate it will decrypt and if it is encrypted with the old cert, it will still decrypt until the expiration date is reached.

1. Open the PHINMS Console

2. Select Configure>>Sender>>General
3. Select Security Category
4. In the Primary Keystore location, enter the path to the new decryption key
5. Enter the password for the new decryption key
6. In the Secondary Keystore location, enter the path to the older decryption key
7. Enter the password
8. Enter the date the old decryption key expires. Format should be: yyyy-mm-dd hh:mm:ss
9. Save
10. Restart PHINMS

9.14 VeriSign LDAP Functionality

When LDAP was enabled on previous versions of PHINMS, the application performed a lookup to VeriSign LDAP Services for the data encryption public key and would append the encryption for each message. This constant VeriSign LDAP lookup would periodically fail if the VeriSign LDAP sever is not reachable. The LDAP service outage would prevent messages from sending until the outage recovered.

To minimize the VeriSign LDAP dependency, the LDAP lookup feature is re-architected in this relese. In his 2.8.02 verision, the PHINMS application has been enhanced to perform a single lookup and then cache the certificate and the expiration date. To maintain secure computing practices, PHINMS performs daily lookups to VeriSign's CRL (Cert Revocation List) Servers to ensure the cached certificate has not been revoked. The use of the VeriSign CRL Services provides the industry standard security measures for certificate usage

1. Open the PHINMS Console
2. Select Configure>>Sender>>General
3. Select the LDAP Category
4. Check Use LDAP Key Retrieval
5. Save
6. Restart PHINMS